Manuel de l’utilisateur

SW-26210

24 ports PoE + 2 ports à commutateur intelligent Web

Marque de commerce

Droits d'auteur © i³ International Inc. 2012.

Contenu sujet à changement sans préavis.

Toutes les autres marques de commerce appartiennent à leurs propriétaires respectifs.

Responsabilité limitée

i³ International ne garantit pas que le matériel fonctionnera correctement dans tous les environnements et avec toutes les applications, et n'offre aucune garantie et représentation, implicite ou explicite, en respect à la qualité, la performance, la commerciabilité ou l'aptitude pour une tâche particulière. i³ International a fait tous les efforts pour s'assurer que ce manuel est exact; i³ International se dégage de toute responsabilité pour toute inexactitude ou omission qui auraient pu se produire. L'information contenue dans ce Manuel de l'Utilisateur est sujette à changement sans préavis et ne représente pas un engagement de la part de i³ International. i³ International n'assume aucune responsabilité pour toutes inexactitudes que pourrait contenir ce Manuel de l'Utilisateur. i³ International ne s'engage pas à mettre à jour ou à conserver à jour l'information dans ce Manuel de l'Utilisateur, et se réserve le droit de faire des améliorations à ce Manuel de l'Utilisateur et/ou aux produits décrits dans ce Manuel de l'Utilisateur, à tout moment sans préavis.
Si vous trouvez, dans ce manuel, de l'information incorrecte, trompeuse ou incomplète, nous aimerions recevoir vos commentaires et suggestions.

Avertissement de la FCC

Cet équipement a été testé et jugé conforme aux limites d’un dispositif numérique de classe A, conformément à la partie 15 de la réglementation de la FCC. Ces limites sont désignées Ces limites existent afin de fournir une protection raisonnable contre une interférence nuisible lorsque l’équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l’énergie de fréquence radio et, s’il n’est pas installé et utilisé conformément au manuel d’instruction, peut causer des interférences nuisibles aux communications radio. Cependant, il n’y a aucune garantie que l’interférence ne se présentera pas dans une installation particulière. Si cet équipement cause effectivement des interférences nuisibles à la réception radio ou télévision, ce qui peut être déterminé en allumant et éteignant l’équipement, on encourage l’utilisateur d’essayer de corriger l’interférence en effectuant une ou plusieurs de ces mesures :

Réorienter ou relocaliser l’antenne de réception.

Augmenter la distance de séparation entre l’équipement et le récepteur.

Connecter l’équipement dans une prise sur un circuit qui est différent de celui sur lequel le récepteur est branché.

Consulter le marchand ou demander l’aide d’un technicien radio/TV expérimenté.

Avertissement de marque CE

Ceci est un produit de classe A. Dans un environnement domestique, ce produit peut causer des interférences radio, pour

lesquelles l'utilisateur pourrait devoir apporter des mesures correctives

Révision

i³ international 24-Port 10/100 Base T avec 2 manuels de l’utilisateur du commutateur intelligent Web RJ-45/SFP 10/100/1000 Base T

POUR LE MODEL : SW-26210

RÉVISION : 1.0

Table des matières

Table des matières 4

1. INTRODUCTION 9

1.1. Aperçu du produit 9

1.2 Caractéristiques du produit 9

Gestion Web 9

2. INSTALLATION 11

2.1. Installation du périphérique 11

2.1.1 Contenu de l'emballage 11

2.1.2 Description du matériel 12

2.1.2. Installation du périphérique 13

3. CONFIGURATION DU LOGICIEL 14

3.1. Connexion 14

3.2. Administration 15

3.2.1. Administrateur 15

3.2.2. Configuration IP du système 16

3.2.3. Statut du système 16

3.3. Paramètres d'usine 17

3.3.1. Réinitialisation du logiciel 17

3.3.2. Réinitialisation du périphérique 18

3.4. Mise à jour du micro logiciel (« Firmware Update ») 18

3.5. Redémarrer 19

3.6. Déconnexion 19

4. GESTION DU PORT 20

4.1. Configuration du port 20

4.1.1 Négociation automatique 20

4.2. Mise en miroir du port 22

4.3. Contrôle de la bande passante 23

4.3.1. « *Broadcast Storm Control* » (Contrôle de l'excès des émissions) 24

4.4. Paramètres PoE 25

4.4.1. Introduction au PoE 25

5. CONFIGURATION DU VLAN 27

5.1. Introduction au VLAN 27

5.1.2. Standard IEEE 802.1Q 27

5.2. Configuration VLAN 29

5.2.1. Mode VLAN 29

5.2.2. Membre VLAN 30

5.3. Configuration de multi à 1 33

6. COMPTEUR PAR PORT 34

Compteur du port 34

7. PARAMÈTRE QoS 35

7.1. À propos de QoS 35

7.2. Configurer la QoS 35

7.2.1. Mode de priorité 36

7.2.2. Port, 802.1p, basé sur IP/DS 36

8. SÉCURITÉ 38

8.1. Contrainte d'adresse MAC 38

8.2. Filtre TCP/UDP 39

9. « SPANNING TREE PROTOCOL » 40

9.1. Paramètres du pont STP 41

9.2. Paramètres du port STP 42

9.3. Paramètres de détection du bouclage 42

10. GROUPAGE DE PORTS (« TRUNKING ») 44

11. SAUVEGARDE / RESTAURATION 46

12. PARAMÈTRES DIVERS 47

13. DÉPANNAGE 48

APPENDICE A : PÉRIPHÉRIQUE RÉSEAU 50

A.1. Affectation des pins RJ-45 50

A.2. 10/100Mbps, 10/100Base-TX 50

ANNEXE B: Store-and-Forward 53

APPENDICE C : Aperçu du PoE 54

C.1. Architecture système AvE (PoE) 54

C.1.1. Transfert d'alimentation via un câble Ethernet CAT5 54

C.2. Processus d'approvisionnement AvE (PoE) 56

C.2.1. Détection de ligne 56

C.2.2. Classification 56

C.2.3. Démarrage 57

C.2.4. Opération 57

C.2.5. Surcharge de puissance 57

C.3. Scénarios de déconnexion de l'alimentation 57

APPENDICE D : GLOSSARY 59

A **59**

Agrégation 59

D **59**

DEI 59

DHCP 59

Relais DHCP 59

Surveillance DHCP 60

DNS 60

I **60**

IEEE 802.1X 60

IGMP 60

Interrogateur IGMP 61

IP 61

Gardien de source IP 61

L **61**

LACP 61

LLDP 62

LLDP-MED 62

M **62**

MAC Table (Table MAC) 62

Mirroring (miroir) 62

N **63**

Négociation automatique 63

P **63**

PD 63

PHY 63

PING 63

PoE 63

Policier 64

Port de routeur 64

Priorité de la balise 64

Q **64**
QCE 64
QCL 64
QoS 64
R **65**
RSTP 65
S **65**
SHA 65
STP 65
T **65**
TCP 65
ToS 66
U **66**
UDP 66
Priorité de l'utilisateur 67
V **67**
VLAN 67
VLAN ID 67
VLAN Privé 67

1. INTRODUCTION

1.1. Aperçu du produit

Ce commutateur fournit des ports 24 10/100Mbps RJ-45, comprend la fonction de détection de croisement MDI / MDIX automatique et peut supporter 2 Combo Gigabit RJ-45/SFP de liaison montante. Vingt-quatre de ces ports offrent des fonctionnalités PoE, offrant le choix ultime de flexibilité du réseau. Grâce à cette fonctionnalité PoE ajoutée, ce commutateur est une solution idéale pour la construction d’une surveillance IP sans fil et de réseaux VoIP.

Il fournit également une fonction VLAN de balise basée sur le port et 802.1q afin d’offrir une meilleure gestion de la circulation, réduire la latence, améliorer la sécurité et économiser la bande passante sans ajout de matériel sur le réseau.

Le but de ce manuel est de fournir à l'utilisateur les connaissances nécessaires pour déployer correctement et en toute sécurité la technologie de réseau en utilisant ce commutateur.

1.2 Caractéristiques du produit

Gestion Web

- Gestion du port
  - Configuration du port
  - Mise en miroir du port
  - Contrôle de la bande passante
  - « Broadcast Strom Control »
  - Configuration On/Off (marche/arrêt) PoE
- Configuration VLAN
  - Basé sur le port / basé sur la balise
  - ID VLAN : 1~4094
- Groupage de ports (« Trunking »)
  - Configuration de l’agrégation des liaisons
  - 2 groupes (1~4 ports pour chaque groupe)
- Configuration QoS
  - Mode prioritaire
  - Classe de la configuration du service
  - TCP/UDP basé sur le port

- Configuration de la sécurité
  - Filtrage de l'adresse MAC
  - Filtrage du port TCP/UDP
- STP/RSTP
- « Spanning Tree Protocol »
- Configuration de la récupération de sauvegarde

Spécifications

- Standards
  - IEEE 802.3 10BaseT
  - IEEE 802.3u 100BaseTX
  - IEEE 802.ab 1000BaseT
  - IEEE 802.3z 1000BaseSX/LX
  - IEEE 802.3x Full-duplex et contrôle du flux
  - IEEE 802.at PoE
  - IEEE 802.3ad Agrégation de liaison
  - IEEE 802.1d « Spanning tree protocol »
  - IEEE 802.1w « Spanning tree protocol » rapide
  - IEEE 802.1x Contrôle de l'accès réseau basé sur le port
  - IEEE 802.1Q VLAN
  - IEEE 802.1p Classe de service
- Nombre de ports
  - 24 ports 10/100BaseTX avec PoE
  - 2 ports Combo Gigabit uplink (RJ-45/SFP)

Mécanique

- Indicateur LED
  - Par port : Liaison/Acte
  - Port PoE : Acte/Statut
  - Par unité : Alimentation
- Consommation d'énergie : 390 Watts (Maximum)
- Alimentation à l'entrée : 100~240V/AC, 50~60HZ
- Alimentation à la sortie : 48V/DC par sortie de port –30W Maximum par port
- Dimensions/poids du produit
  - 45 × 440 × 330 mm (H × W ×D) / 4.6kg

Performance

- Adresse MAC : 4K
- La mémoire tampon : 2.75Mb
- Méthode de transmission : Stockage et retransmission

2. INSTALLATION

Cette section décrit les caractéristiques et l’installation du matériel du commutateur intelligent SW-26210. Pour faciliter le contrôle et la gestion, familiarisez-vous avec ses indicateurs d'affichage et ses ports. Assurez-vous de lire chaque chapitre en entier avant de le connecter avec quelconque dispositif réseau.

2.1. Installation du périphérique

2.1.1 Contenu de l’emballage

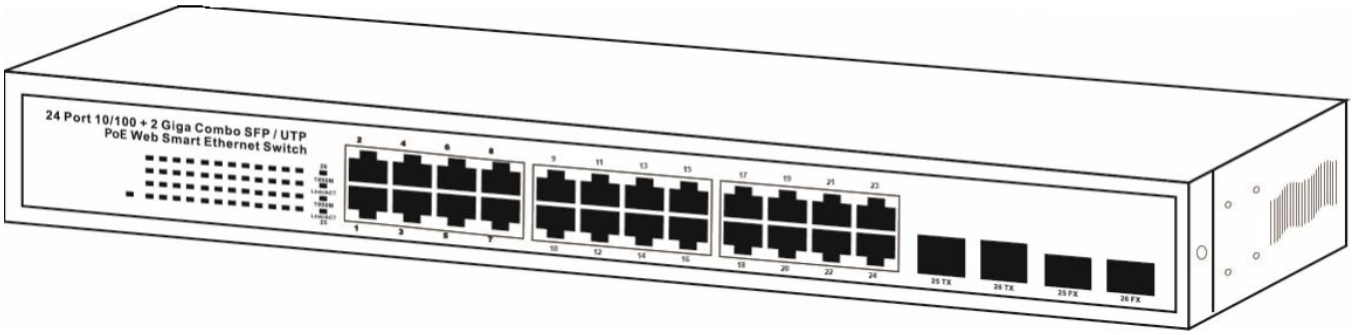


Figure 1 – commutateur SW-26210

Avant d’installer ce commutateur, vérifiez que votre paquet contienne les items suivants :

- Le commutateur SW-26210
- Le fil d’alimentation
- Le disque compact du manuel d’utilisateur
- Le kit de montage du support

Si l'un de ceux-ci sont manquants ou endommagés, s'il vous plaît, veuillez contacter votre revendeur immédiatement, si possible, conservez la boîte de carton comprenant l'emballage d'origine et utilisez-le pour remballer le produit dans le cas où il est nécessaire de le retourner pour effectuer une réparation.

2.1.2 Description du matériel

Dimensions/poids physiques

45 × 440 × 330 mm (H × W ×D) / 4.6kg

Panneau avant

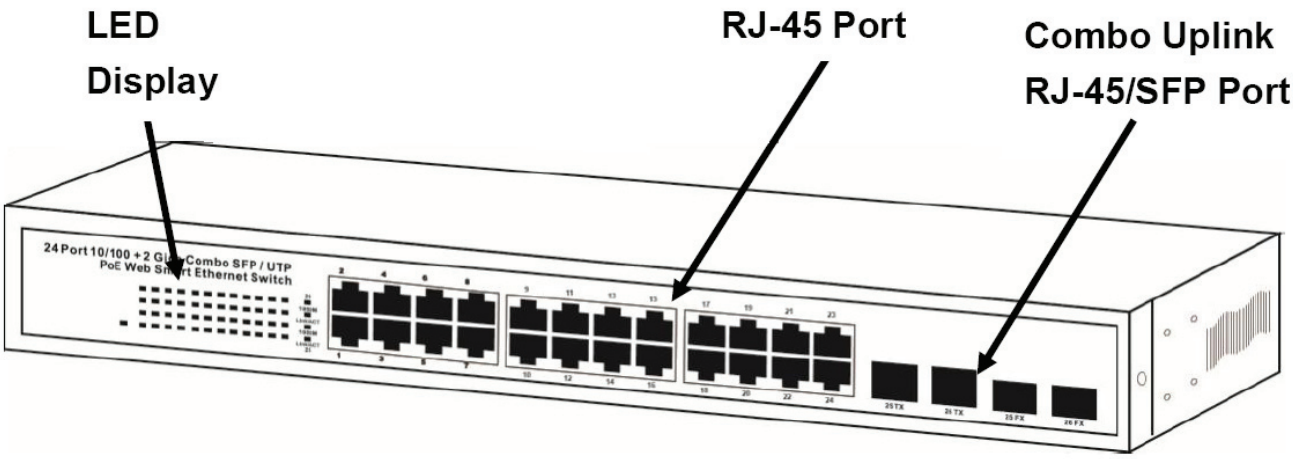


Figure 2 – Aperçu du panneau avant

Le panneau avant du commutateur intelligent Web comprend 24 ports 10/100Base-TX RJ-45 et 2 ports combo gigabit uplink RJ-45/SFP. Les indicateurs LED sont aussi localisés sur le panneau avant.

Indicateurs LED

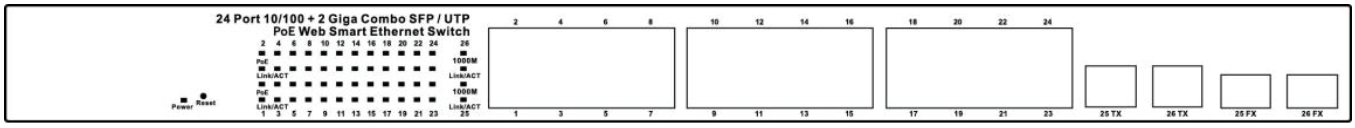


Figure 3 – Aperçu du panneau avant

Les indicateurs LED présentent l'information en temps réel du statut d'opération systématique. Le tableau suivant donne la description des statuts LED ainsi que leur signification.

LED	Statut	Description	Étiquette
Alimentation	Marche	Interrupteur d'alimentation marche/arrêt	Alimentation
1000M	Marche	Transmission du lien à 1000 Mbps	2 (25-26)

	Arrêt	Link transmission at 10/100 Mbps	
Lien/ACT	Marche	Lien	26 (1~26)
	Clignotant	Activation des données	
PoE	Marche	Le port est en liaison avec le dispositif alimenté	24 (1~24)
	Arrêt	Pas de dispositif alimenté connecté	

Tableau 1 – Descriptions des statuts LED

Panneau arrière

La prise d’alimentation à 3 axes est placée sur le côté droit en bas du panneau arrière du commutateur comme indiqué ci-dessous.

Figure 4 - Back panel overview

2.1.2. Installation du périphérique

Posez le commutateur sur une grande surface plane avec une prise électrique tout près. La surface plane devrait être propre, lisse, au niveau et stable. Assurez-vous qu’il y ait assez d’espace vertical autour du commutateur pour permettre branchement de câbles, du fils d’alimentation et pour permettre la circulation d’air. Utilisez le câble à paire torsadée pour connecter ce commutateur à votre PC.

3. CONFIGURATION DU LOGICIEL

Cette section décrit la configuration du logiciel du commutateur SW-26210 utilisant l'interface Web.

3.1. Connexion

Ouvrez un navigateur Web et entrez l'adresse ***192.0.0.20***. Une fenêtre de connexion apparaîtra.

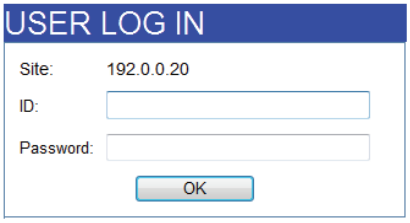


Figure 5 – Fenêtre de connexion

Par défaut, l'ID sera admin. Entrez le mot de passe pour vous authentifier. Ensuite, cliquez sur OK. Le processus de connexion est complété si le message "Password successfully entered" apparaît. Entrez le nom d'utilisateur et le mot de passe. Si ceci est la première connexion, les éléments d'identification par défaut sont :

ID: admin

Mot de passe : ***admin***

Après l'authentification, "Password successfully entered" apparaîtra et vous serez redirigé vers la page principale.

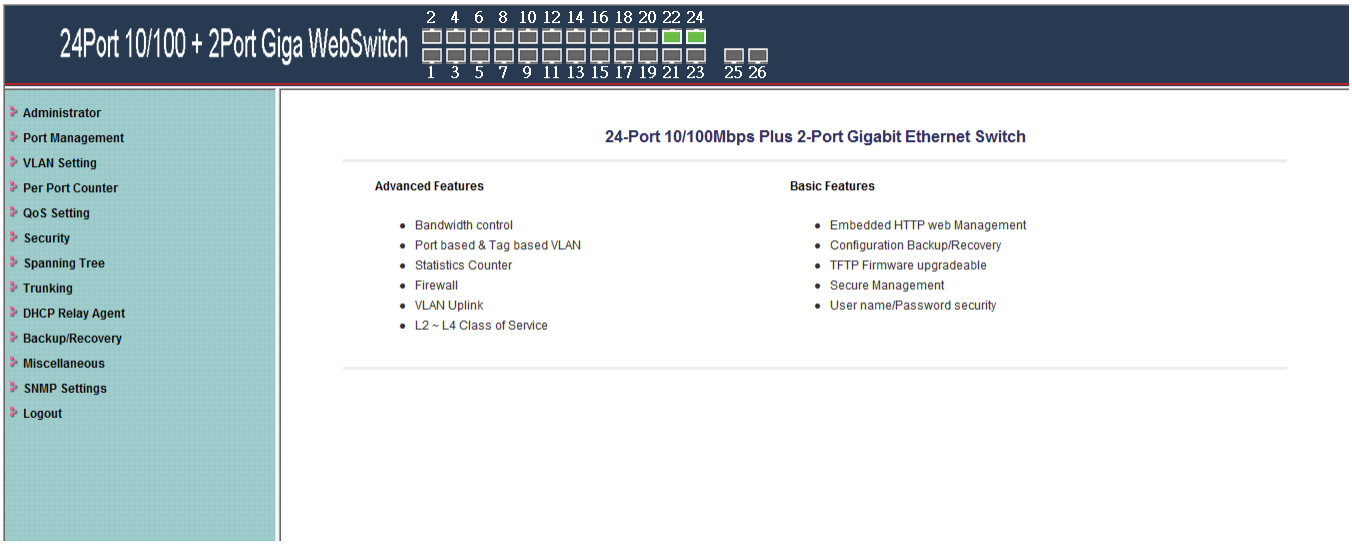


Figure 6 – Page principale de l'interface Web

Sinon, ce message apparaîtra :

Figure 7 – Erreur de connexion

3.2. Administration

3.2.1. Administrateur

Cliquer sur ***Administrator,*** dans la zone de navigation, fera apparaître les options administratives sur la zone principale. Si ceci est votre première connexion, changez le nom d'utilisateur et le mot de passe dans la section de la configuration de l'authentification.

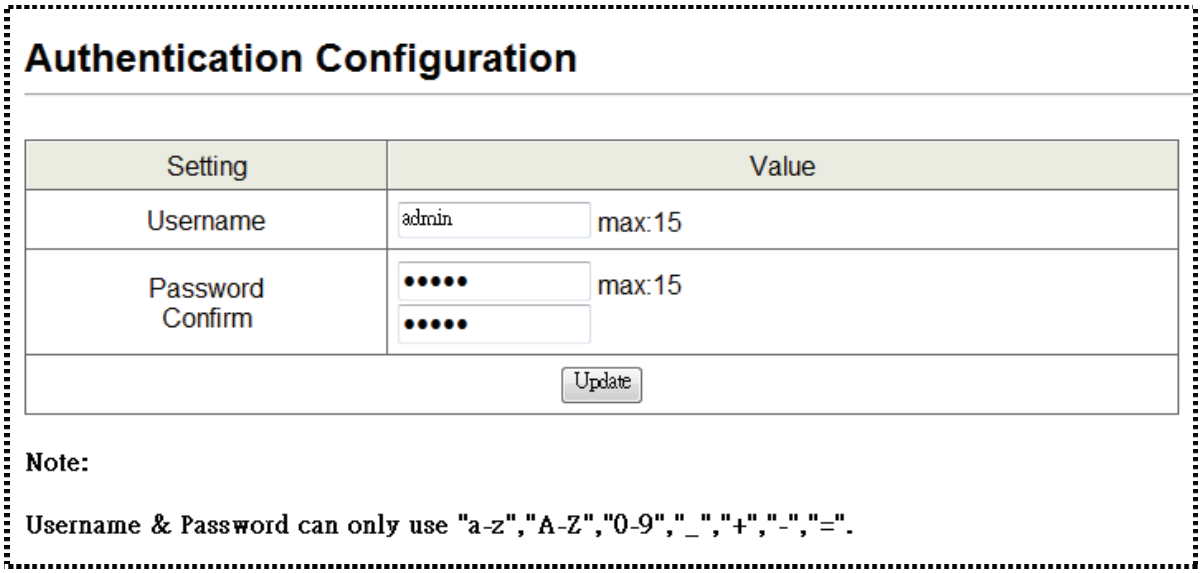


Figure 8 – Configurer le nom d'utilisateur et le mot de passe

3.2.2. Configuration IP du système

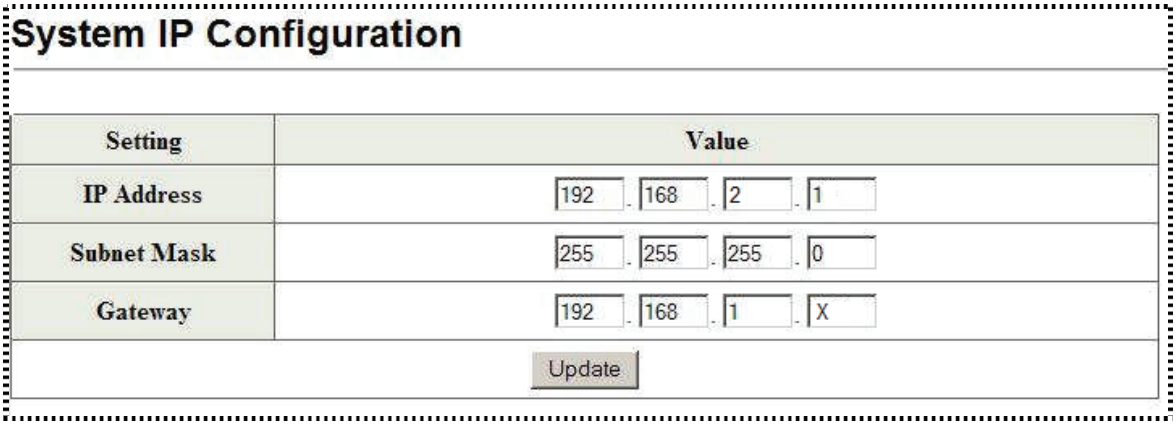


Figure 9 - Configurer l'IP du commutateur

Cette page règle l'information sur la configuration du système incluant l'adresse IP, le masque sous-réseau et la passerelle courants. Les paramètres sont comme ceci :

- IP address: Assigne manuellement l'adresse IP au commutateur. L'adresse IP par défaut est ***192.0.0.20.***
- Subnet Mask: Assigne le masque sous-réseau à l'adresse IP.
- Gateway: Assigne la passerelle réseau.

Cliquez **Update** pour sauvegarder vos changements. Remarque : Changer l'adresse IP requiert le redémarrage.

3.2.3. Statut du système

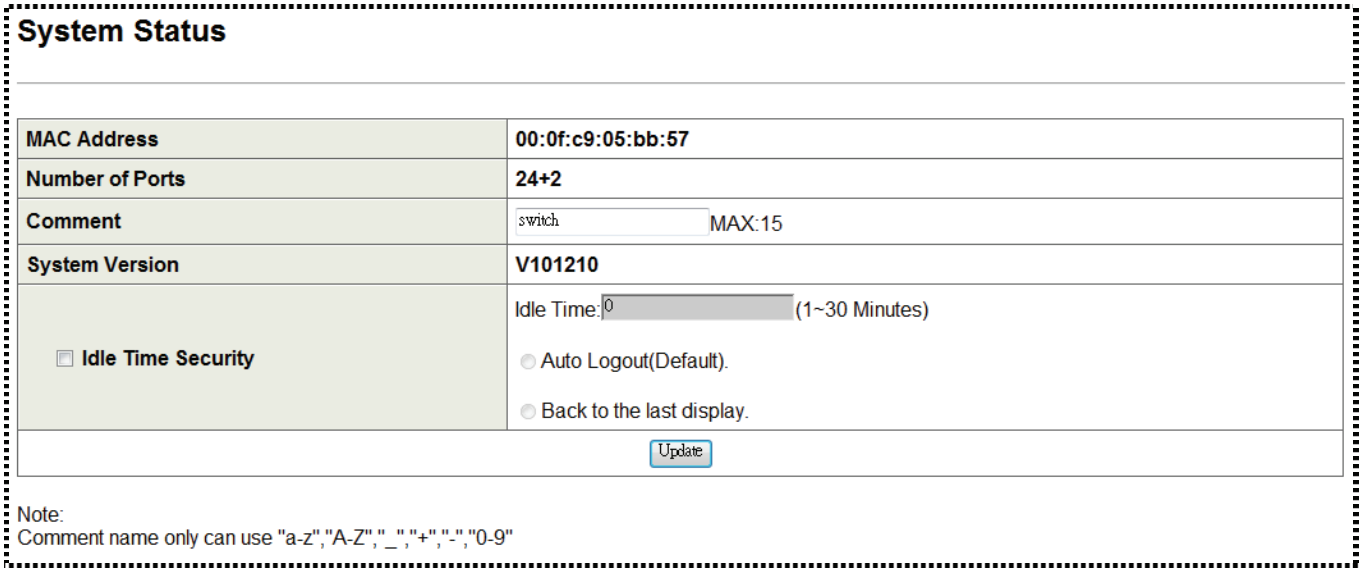


Figure 10 – Un aperçu du commutateur

Cette page affiche l'information de base à propos du commutateur.

- MAC Address: Affiche l'adresse unique du périphérique assignée par le manufacturier (par défaut).
- Number of Ports: Affiche le nombre de ports dans le commutateur.
- Comment: Ce champ peut être utilisé pour prendre des notes. Il est permis d'écrire un maximum de 15 caractères.
- System Version: Affiche la version du micro logiciel du commutateur.
- Idle Time Security: Lorsque l'interface web est immobile pour un certain temps, le logiciel effectuera la déconnexion automatique ou retourner à l'affichage précédant. Réglez un **Idle time** dans le champ correspondant. Cliquez sur **Auto Logout (Default)** pour éteindre le commutateur lorsque l'interface est immobile pour un temps spécifié. Cliquez **Back to the last display** pour retourner à la dernière fenêtre lorsque l'interface est immobile pour un temps spécifié. Cliquez sur **Update** pour sauvegarder les changements.

3.3. Paramètres d'usine

3.3.1. Réinitialisation du logiciel

Cliquez sur le bouton **Load** pour faire revenir le commutateur à ses configurations d'usine originales avec l'exception du nom d'utilisateur, du mot de passe et de la configuration IP.

Figure 11 – Réinitialisation des paramètres par défaut à l'usine

Si vous désirez également reconfigurer le nom d'utilisateur, le mot de passe, les paramètres de configuration IP, pressez le bouton physique (réel) « reset » sur le commutateur.

3.3.2. Réinitialisation du périphérique

Pressez sur le bouton physique « reset » sur le commutateur pour retourner aux paramètres d'usine originaux incluant les paramètres qui ne sont pas couverts par la réinitialisation du logiciel.

(1) Pour activer, pressez sur le bouton « reset » d'usine pendant cinq secondes jusqu'à ce que le LED commence à clignoter.

(2) Le LED clignotant signale que le CPU est en train d'exécuter la procédure de réinitialisation. Relâchez le bouton.

Après avoir complété cette procédure, tous les paramètres d'usine seront restaurés incluant l'adresse IP, le nom d'utilisateur, le mot de passe ainsi que tous les autres paramètres du commutateur.

3.4. Mise à jour du micro logiciel (« Firmware Update »)

Avant de faire la mise à jour du micro logiciel du commutateur, il est recommandé d'effacer la mémoire flash du commutateur. Le chargeur de démarrage demeurera intact à l'aide d'un mécanisme d'autoprotection qui assure un fonctionnement correct même s'il y a une coupure de l'alimentation ou une défaillance du réseau durant la mise à jour.

Firmware Update
Please input the password to continue the Firmware Update process.
Password
ReConfirm
Update
Notice:After clicking the "UPDATE" button, IF the firmware update webpage is not redirected correctly or is shown as "Webpage not found". Please connect to http://192.168.2.1

Figure 12 – Confirmer la mise à jour du micro logiciel

Entrez votre mot de passe et confirmez-le dans les champs appropriés. Cliquez **Update**. Cette fenêtre apparaîtra.

Firmware Update by Web
Select the image file:
Browse...
UPDATE
If the update process somehow goes wrong(Ex: power failure), please connect to http://192.168.2.1 to restart.(If possible, reset device first.)
Firmware Update by TFTP
(TFTP client)Use MS Windows' Command Prompt window to run tftp client program.
Syntax: c:\tftp -i 192.168.1.1 put FILE_DIRECTORY\FILENAME.bin

Figure 13 - Select an update file

Click **Browse...** to select the new firmware image and Click **Update** to save your changes.

3.5. Redémarrer

Pour effectuer une réinitialisation douce, cliquez sur **Confirm** pour réinitialiser le dispositif. Pour effectuer une réinitialisation sévère, utilisez le bouton par défaut d'usine sur le commutateur.

Figure 14 – Confirmer pour réinitialiser

3.6. Déconnexion

À tout moment, cliquez sur le lien Logout dans la zone de navigation pour vous déconnecter de l'interface web.

4. GESTION DU PORT

La gestion du port comprend la configuration et la mise en miroir du port, le contrôle de la bande passante, le « Broadcast Storm Control » et le PoE.

4.1. Configuration du port

Pour accéder aux options de la configuration du port, cliquez sur le lien ***Port Configuration*** dans la panneau de navigation de l'interface web.

4.1.1 Négociation automatique

La négociation automatique règle automatiquement la meilleure bande passante possible lorsqu'une connexion est établie avec un autre dispositif réseau (habituellement à « Power On » ou « Reset »). Cela se fait en détectant les modes et les vitesses avec lesquelles les deux dispositifs connectés sont capables de fonctionner. Les deux dispositifs, 10Base-T et 100Base-TX, peuvent se connecter avec le port soit dans le mode *Half-* ou *Full-Duplex*.

Si le dispositif attaché est :	100Base-TX port will set to:
10Mbps, pas de négociation automatique	10Mbps.
10Mbps, avec négociation automatique	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, pas de négociation automatique	100Mbps
100Mbps, avec négociation automatique	100/200Mbps (100Base-TX/Full-Duplex)

Tableau 2 – Résumé de la négociation automatique

Dans la configuration du port, vous pouvez régler et voir le mode d'opération pour chaque port. Cochez la boîte près du numéro du port pour voir ou modifier les paramètres actuels. Configurez les ports en utilisant les menus déroulants dans le haut.

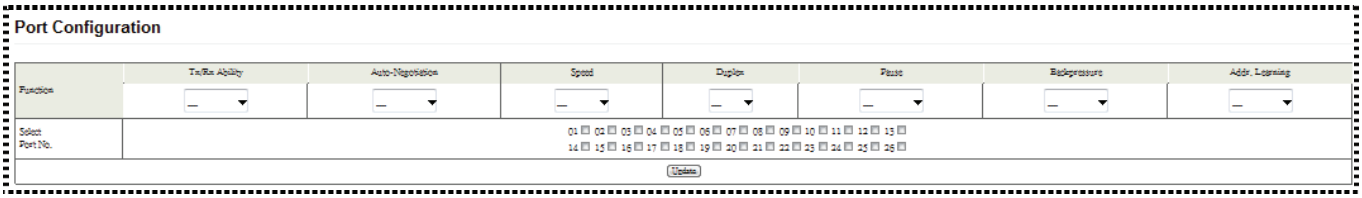


Figure 15 – Configurer les paramètres de négociation automatique

- Select Port No.: Cochez les boîtes près du numéro du port qui est à configurer.

Les paramètres sont :

- Auto-Negotiation: Sélectionnez ***Enable*** ou ***Disable***. Si ***Enable*** est sélectionné, la vitesse, le mode Duplex, la pause, la «back pressure, la capacité TX et l'apprentissage d'adresse sont négociés automatiquement. Si ***Disable***, ces paramètres doivent être assignés manuellement.
- Speed: Lorsque la négociation automatique est désactivée, la vitesse doit être spécifiée manuellement.
- Duplex: Lorsque la négociation automatique est désactivée, le mode de connexion, soit ***Half*** ou ***Full***, doit être spécifié.
- Pause: Le contrôle du flow pour la connexion à une vitesse de 10/100Mbps en mode ***Full-duplex***.
- Backpressure: Le contrôle du flow pour la connexion à une vitesse de 10/100Mbps en mode ***Half-duplex***.
- TX/RX Capability: Lorsque la négociation automatique est désactivée, les utilisateurs doivent activer ou désactiver manuellement TX/RX.
- Addr. Learning: Lorsque la négociation automatique est désactivée, les utilisateurs doivent activer ou désactiver manuellement l'apprentissage d'adresse.
- L'affichage montre les informations suivantes :
- Current Status: Affiche le statut actuel du port.
- Setting Status: Affiche le statut actuel.

Cliquez sur **Update** pour enregistrer vos modifications. Un tableau, au bas du panneau principal, affiche un résumé de chaque configuration de chaque port.

Port	Current Status				Setting Status						
	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	Auto-Nego	Speed	Duplex	Pause	Backpressure	Addr. Learning
1	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
2	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
3	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
4	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
5	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
6	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
7	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
8	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
9	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
10	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
11	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
12	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
13	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
14	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
15	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
16	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
17	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
18	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
19	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
20	●	100M	FULL	ON	ON	AUTO	100M	FULL	ON	ON	ON
21	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
22	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
23	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
24	---	---	---	---	ON	AUTO	100M	FULL	ON	ON	OFF
25	---	---	---	---	ON	AUTO	1G	FULL	ON	ON	OFF
26	---	---	---	---	ON	AUTO	1G	FULL	ON	ON	OFF

Figure 16 – Statut du port

4.2. Mise en miroir du port

Configurez la mise en miroir du port sur cette page. Cette fonction surveille le trafic réseau qui fait suivre une copie de chaque paquet entrant et sortant à partir d'un port d'un commutateur réseau vers un autre port où le paquet peut être étudié. Cela permet à l'administrateur de garder l'œil ouvert sur la performance du commutateur et de l'altérer si nécessaire.

Port Mirroring

Dest Port	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐	8 ☐	9 ☐	10 ☐	11 ☐	12 ☐	13 ☐
	14 ☐	15 ☐	16 ☐	17 ☐	18 ☐	19 ☐	20 ☐	21 ☐	22 ☐	23 ☐	24 ☐	25 ☐	26 ☐
Monitored Packets	Disable ▾												
Source Port	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	6 ☐	7 ☐	8 ☐	9 ☐	10 ☐	11 ☐	12 ☐	13 ☐
	14 ☐	15 ☐	16 ☐	17 ☐	18 ☐	19 ☐	20 ☐	21 ☐	22 ☐	23 ☐	24 ☐	25 ☐	26 ☐
Update													
Multi to Multi Sniffer function													

Figure 17 – Configure port mirroring

Les paramètres pour ce paramètre sont :

- Destination (mirroring) port: Pour surveiller le trafic RX ou le trafic TX, ou les deux à partir du port source. La mise en miroir des ports peut être connectée à un analyste LAN ou *Netxray*.
- Monitored Packets: Déroulez le menu déroulant pour sélectionner entre RX, TX ou bien RX et TX.
- Source Port: Sélectionnez les ports à surveiller. Tout le trafic des ports surveillés sera copié vers le port (destination) de la mise en miroir. Sélectionnez des ports à multiple source en cochant la boîte en-dessous de l'étiquette du numéro de port à être mis en miroir.

Cliquez sur **Update** pour enregistrer vos modifications

4.3. Contrôle de la bande passante

Configurer la bande passante allouée sur cette page. Le taux TX et Rx est un nombre qui va de ***1*** à ***255***. Ce nombre devrait être multiplié par la résolution de la bande passante sélectionnée afin d'obtenir la bande passante réelle.

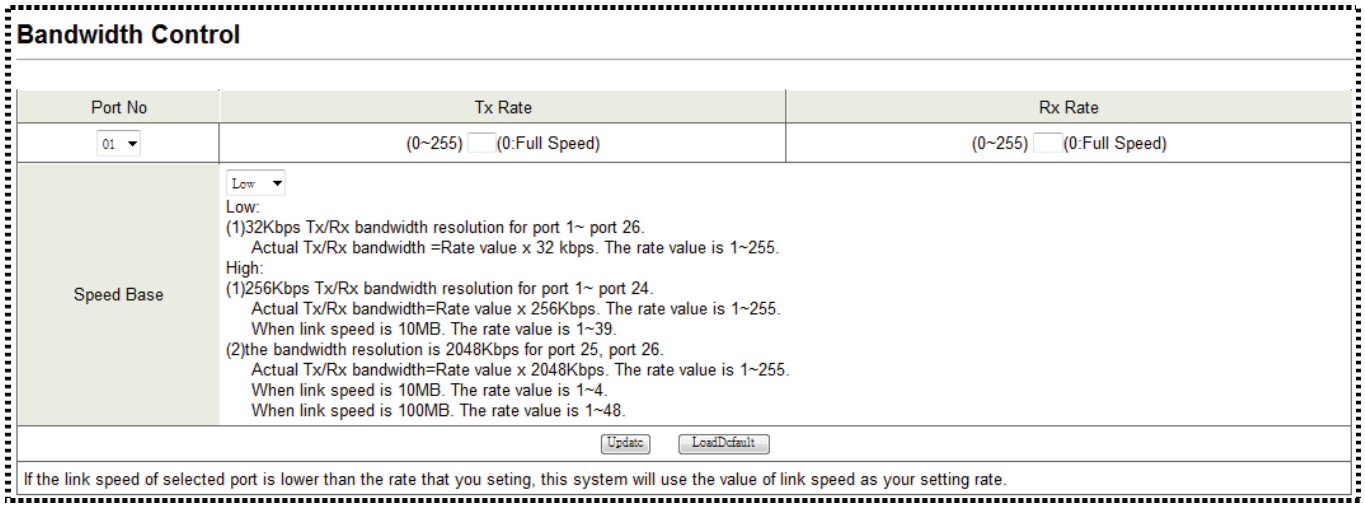

Bandwidth Control
Port No
Tx Rate
Rx Rate
01
(0~255) (0:Full Speed)
(0~255) (0:Full Speed)
Low
Speed Base
Low:
(1)32Kbps Tx/Rx bandwidth resolution for port 1~ port 26.
Actual Tx/Rx bandwidth =Rate value x 32 kbps. The rate value is 1~255.
High:
(1)256Kbps Tx/Rx bandwidth resolution for port 1~ port 24.
Actual Tx/Rx bandwidth=Rate value x 256Kbps. The rate value is 1~255.
When link speed is 10MB. The rate value is 1~39.
(2)the bandwidth resolution is 2048Kbps for port 25, port 26.
Actual Tx/Rx bandwidth=Rate value x 2048Kbps. The rate value is 1~255.
When link speed is 10MB. The rate value is 1~4.
When link speed is 100MB. The rate value is 1~48.
Update
LoadDefault
If the link speed of selected port is lower than the rate that you seting, this system will use the value of link speed as your setting rate.

Figure 18 – Régler la bande passante permise

Un sommaire de l'usage de la bande passante est affiché plus bas.

Port No.	Tx Rate	Rx Rate	Link Speed	Port No.	Tx Rate	Rx Rate	Link Speed
1	Full Speed	Full Speed	---	14	Full Speed	Full Speed	---
2	Full Speed	Full Speed	---	15	Full Speed	Full Speed	---
3	Full Speed	Full Speed	---	16	Full Speed	Full Speed	---
4	Full Speed	Full Speed	---	17	Full Speed	Full Speed	---
5	Full Speed	Full Speed	---	18	Full Speed	Full Speed	---
6	Full Speed	Full Speed	---	19	Full Speed	Full Speed	---
7	Full Speed	Full Speed	---	20	Full Speed	Full Speed	100M
8	Full Speed	Full Speed	---	21	Full Speed	Full Speed	---
9	Full Speed	Full Speed	---	22	Full Speed	Full Speed	---
10	Full Speed	Full Speed	---	23	Full Speed	Full Speed	---
11	Full Speed	Full Speed	---	24	Full Speed	Full Speed	---
12	Full Speed	Full Speed	---	25	Full Speed	Full Speed	---
13	Full Speed	Full Speed	---	26	Full Speed	Full Speed	---

Figure 19 – Sommaire de la bande passante

4.3.1. « *Broadcast Storm Control* » (Contrôle de l'excès des émissions)

Le commutateur met en œuvre un mécanisme de contrôle de l'excès des émissions. Cochez les ports dans la rangée **Enable Port** pour sélectionner les ports qui supprimeront les paquets d'émissions entrantes si le nombre de paquets d'émissions reçu atteint la limite prédéfinie. Chaque fonction de protection contre l'excès des émissions du port peut être activée individuellement.

Broadcast Storm Control

Threshold	63 1~63											
Enable Port	1	2	3	4	5	6	7	8	9	10	11	12	13
	14	15	16	17	18	19	20	21	22	23	24	25	26

Update

This value indicates the number of broadcast packet which is allowed to enter each port in one time unit. One time unit is 50us for Gigabit speed, 500 us for 100Mbps speed and 5000us for 10Mbps speed

Note: This effect may be not significant for long broadcast packet, since the broadcast packet count passing through the switch in a time unit is probably less than the specified number.

Figure 20 – Écran du contrôle de l'excès des émissions (Broadcast storm control)

Les paquets d'émissions ne sont vérifiés que dans les ports sélectionnés. L'émission est réglée à 500 us pour une vitesse de 10Mbps et 5ms pour une vitesse de 100Mbps. Les paquets d'émissions en excès seront rejetés. Les paquets d'un port non sélectionné sont traités comme faisant partie d'un trafic normal.

- Threshold: Tapez une limite allant de ***1*** à ***63*** pour limiter le nombre maximal d'octets qu'un port peut envoyer ou recevoir durant

une certaine période de temps.

- Enable Port: Les ports qui sont cochés arrêteront de transmettre ou de recevoir des données lorsque les limites qui leurs sont données dans Threshold sont atteintes. Les ports qui ne sont pas cochés fonctionneront normalement.

Cliquez sur **Update** pour enregistrer vos modifications.

4.4. Paramètres PoE

Plusieurs paramètres PoE peuvent être réglés ici. Pour de plus amples informations, lisez l’appendice C à la section « Processus d’approvisionnement PoE. »

4.4.1. Introduction au PoE

Basé sur le standard mondial IEEE 802.3af, PoE est une technologie Ethernet câblée. PoE permet à l’énergie électrique nécessaire pour le fonctionnement de chaque dispositif en périphérie (caméras IP, téléphones IP, etc.) d’être transporté par les câbles de données plutôt que par des cordons d'alimentation distincts. Une telle configuration réseau aide les entreprises à améliorer la productivité en réduisant le nombre de fils qui doivent être utilisés pour installer le réseau, engendrant ainsi un coût moindre et des pannes de courant moins courantes. Dans le cas des technologies de surveillance, les caméras IP et les systèmes d'accès peuvent être installés dans une installation sans encourir de coûts associés à l'embauche d'un électricien. Fournissant jusqu'à 24 PoE dans l'interface de ligne de puissance, le commutateur peut facilement construire un système de téléphonique IP, un système de caméra IP ou un groupe AP ayant un contrôle centralisé d’alimentation pour toute l'entreprise. Par exemple, une caméra 24 / AP peut être facilement installée au coin du bâtiment de la compagnie pour ses besoins de surveillance ou on peut construire un environnement sans fil d'itinérance dans le bureau. Sans la limitation de la prise de courant, le commutateur PoE permet l'installation facile et efficace de caméras ou de WLAN AP.

POE Configuration

Port	1	2	3	4	5	6	7	8
Enable	☑	☑	☑	☑	☑	☑	☑	☑
PSE Current	No Load	No Load	No Load	No Load	No Load	No Load	No Load	No Load
Minimun Output Power	---	---	---	---	---	---	---	---
POE Class	---	---	---	---	---	---	---	---
Port	09	10	11	12	13	14	15	16
Enable	☑	☑	☑	☑	☑	☑	☑	☑
PSE Current	No Load	No Load	No Load	No Load	No Load	No Load	No Load	No Load
Minimun Output Power	---	---	---	---	---	---	---	---
POE Class	---	---	---	---	---	---	---	---
Port	17	18	19	20	21	22	23	24
Enable	☑	☑	☑	☑	☑	☑	☑	☑
PSE Current	No Load	No Load	No Load	No Load	No Load	No Load	No Load	No Load
Minimun Output Power	---	---	---	---	---	---	---	---
POE Class	---	---	---	---	---	---	---	---

Update

Update: Update the power control funtion.
Enable☑ :Power On
Enable☐ :Power Off

Figure 21 – Écran de configuration PoE

Cette page affiche l'information PoE à propos du PSE du port, d'un minimum de sortie et de la classe PoE. Cliquez sur **Enable** pour utiliser ce port pour le PoE.

5. CONFIGURATION DU VLAN

5.1. Introduction au VLAN

Un réseau local virtuel (VLAN) est une topologie réseau configurée en fonction d'un schème logique plutôt que d'un endroit physique. Le VLAN peut être utilisé pour combiner n'importe quelle location de segments LAN dans un groupe autonome d'utilisateurs qui apparaît en tant que LAN unique. Le VLAN segmente aussi logiquement le réseau en différents domaines de diffusion de sorte que les paquets soient renvoyés seulement entre les ports à l'intérieur du VLAN. De façon générale, un VLAN correspond à un sous réseau particulier cependant, ceci n'est pas nécessairement le cas.

Le VLAN peut augmenter la performance en conservant la bande passante et améliorer la sécurité en limitant le trafic à des domaines spécifiques.

Les nœuds en périphérie qui communiquent entre eux fréquemment sont assignés au même VLAN, peu importe l'endroit physique qu'ils occupent sur le réseau. De façon logique, un VLAN peut être assimilé à d'un domaine de diffusion parce que les paquets d'émissions sont renvoyés seulement aux membres de ce VLAN sur lequel l'émission a été initiée.

Peu importe la base selon laquelle les nœuds en périphérie ont été uniquement identifiés et les appartenances VLAN de ces nœuds ont été assignées, les paquets ne peuvent pas traverser un VLAN sans dispositif de réseau qui performe une fonction de routeur entre les VLAN.

5.1.2. Standard IEEE 802.1Q

Le VLAN IEEE 802.1Q (balise) est mis en œuvre sur le commutateur. Le VLAN 802.1Q a besoin d'une étiquette, ce qui leur permet de couvrir l'ensemble du réseau (en supposant que tous les commutateurs du réseau sont conformes à la norme IEEE 802.1Q).

Le VLAN permet à un réseau d'être segmenté afin de réduire la taille des domaines de diffusion. Tous les paquets entrant dans un VLAN seront transmis seulement aux commutateurs IEEE 802.1Q compatibles qui sont membres de ce VLAN, y compris les paquets de diffusion, de multidiffusion et de monodiffusion provenant de sources inconnues.

Le VLAN peut également fournir un niveau de sécurité à votre réseau. Le VLAN IEEE 802.1Q délivrera seulement les paquets entre les stations qui sont membres du VLAN. N'importe quel port peut être configuré en tant que balisé ou non-balisé.

- La caractéristique *non-balisé* du VLAN IEEE 802.1Q permet à un VLAN de travailler avec des commutateurs

traditionnels qui ne reconnaissent pas les balises VLAN dans l’entête d’un paquet.

- La caractéristique *balisé* permet au VLAN de couvrir de multiples commutateurs 802.1Q compatibles à travers une connexion physique unique et permet au *Spanning Tree* (L’arborescence) d’être activée et de fonctionner normalement sur tous les ports.

Quelques termes pertinents :

- *Tagging* (baliser) : L’acte de mettre l’information d’un VLAN 802.1Q dans l’entête d’un paquet.
- *Untagging* (non-baliser) : L’acte de dépouiller l’entête d’un paquet de l’information d’un VLAN 802.1Q.

Balises du VLAN 802.1Q

La figure ci-dessous montre la balise VLAN 802.1Q. Il y a quatre octets supplémentaires ajoutés la suite de l'adresse MAC source. Leur présence est indiquée par une valeur de 0x8100 dans le champ de type Ether. Lorsque le champ d'un paquet de type Ether est égal à 0x8100, le paquet porte la balise IEEE 802.1Q/802.1p. La balise est contenue dans les deux octets suivants et est composé trois bits à priorité utilisateur, d’une bit de l'identificateur de format canonique (FCI - utilisé pour encapsuler des paquets *Token Ring* afin qu'ils puissent être transportés à travers l’épine dorsale Ethernet) et de 12 bits de l'ID VLAN (VID). Les trois bits de priorité utilisateur sont utilisées par 802.1p. Le VID est l'identificateur de réseau local virtuel et est utilisé par la norme 802.1Q. C’est parce que le VID est de 12 bits que 4094 uniques VLAN peuvent être identifiés.

La balise est insérée dans l'en-tête du paquet, celle-ci allongeant le paquet entier à plus de 4 octets de long. L'ensemble des informations initialement contenues dans le paquet est conservé.

Le type Ether et l'ID VLAN sont insérés à la suite de l'adresse MAC source mais avant le type/longueur Ether d'origine ou le contrôle du lien logique. Le contrôle de redondance cyclique (CRC) doit être recalculé parce que le paquet est maintenant un peu plus long qu'à l'origine.

ID VLAN du port

Les paquets balisés (transportant l’information 802.1Q VID) peuvent être transmis à partir d’un dispositif réseau 802.1Q conforme vers un autre en maintenant l’information VLAN intacte. Ceci permet aux VLAN 802.1Q de couvrir les dispositifs réseaux ou même le réseau en entier en autant que les dispositifs réseaux sont 802.1Q conformes.

Tous les ports physiques sur un commutateur ont une PVID. Les ports 802.1Q ont également une PVID qui leur est assigné et qu’ils utilisent à l’intérieur du commutateur. S’il n’y a aucune VLAN qui soit définie sur le commutateur, tous les ports ont un VLAN par défaut avec une PVID égale à 1 qui leurs sont assignés. La PVID du port sur lequel ces paquets non-balisés ont été reçus leur est assignée. Les décisions de renvoi se basent sur cette PVID dans la mesure où le VLAN est concerné. Les paquets balisés sont renvoyés en fonction de la VID contenue dans la balise elle-même. Une PVID est aussi assignée à chaque paquet balisé mais la VID est utilisé pour les décisions de renvoi plutôt que la PVID.

Les commutateurs qui sont sensibles à la balise doivent garder un tableau pour lier la PVID à l’intérieur du commutateur à

une VID du réseau. Le commutateur comparera la VID d'un paquet qui doit être transmis à la VID du port qui doit transmettre le paquet. Si les deux VID sont différentes, le paquet est rejeté. Les dispositifs réseaux sensibles ou non à la balise peuvent coexister sur le même réseau à cause de l'existence de la PVID pour les paquets non-balisés et la VID pour les paquets balisés.

Un port de commutateur ne peut avoir qu'une seule PVID mais peut avoir le nombre de VID que la mémoire dans le tableau VLAN de ce commutateur peut stocker.

Parce que certains dispositifs sur un réseau peuvent ne pas être sensibles à la balise, une décision doit être prise avant la transmission des paquets à chaque port sur les dispositifs sensibles à la balise. Si le port de transmission est connecté à un dispositif qui n'est pas sensible à la balise, le paquet devrait être non-balisé. Si le port de transmission est connecté à un dispositif sensible à la balise, le paquet devrait être balisé.

VLAN non-balisés

Les VLAN non-balisés (ou statiques) sont, de façon générale, utilisés pour réduire le trafic d'émissions et pour augmenter la sécurité. Un groupe d'utilisateurs réseau associés à un VLAN forme un domaine d'émissions qui est séparé des autres VLAN configures sur le commutateur. Les paquets sont renvoyés seulement entre les ports qui sont désignés au même VLAN. Les VLAN non-balisés peuvent être utilisés pour isoler manuellement les groupes ou les sous-réseaux d'utilisateurs.

5.2. Configuration VLAN

Pour accéder les options VLAN, cliquez sur le lien VLAN Configuration dans le panneau de navigation de l'interface web.

5.2.1. Mode VLAN

Figure 22 – Basculer entre les modes VLAN

Vous pouvez sélectionner le mode VLAN du commutateur. Les groupes VLAN basés sur le port voyagent sur un commutateur unique. Il n'y a pas de transfert de trafic à l'intérieur des groups VLAN vers d'autres commutateurs. Pour le transfert vers d'autres commutateurs, utilisez un VLAN base sur la balise. Dans le mode VLAN vous pouvez passer d'un VLAN basé sur la balise à un VLAN basé sur le port. Un VLAN basé sur le port est le mode par défaut. Cliquez **Change VLAN mode** pour changer de mode.

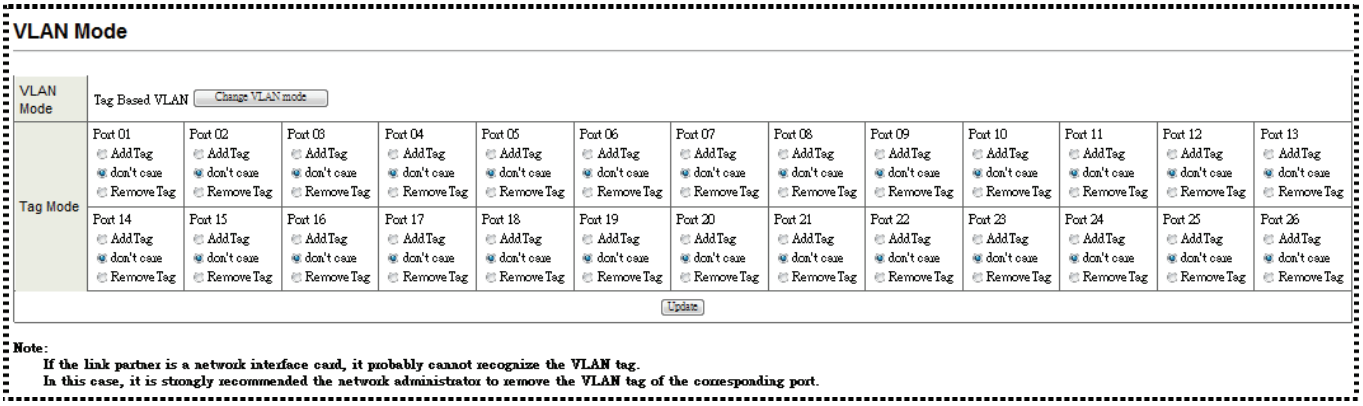

VLAN Mode
VLAN Mode
Tag Based VLAN
Change VLAN mode
Tag Mode
Port 01 Port 02 Port 03 Port 04 Port 05 Port 06 Port 07 Port 08 Port 09 Port 10 Port 11 Port 12 Port 13
Port 14 Port 15 Port 16 Port 17 Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24 Port 25 Port 26
Add Tag
don't care
Remove Tag
Update
Note:
If the link partner is a network interface card, it probably cannot recognize the VLAN tag.
In this case, it is strongly recommended the network administrator to remove the VLAN tag of the corresponding port.

Figure 23 – Sélectionner les options pour le VLAN

Sur cet écran, vous pouvez maintenant définir et configurer vos ports pour les liaisons montantes et descendantes. Ceux-ci sont importants puisque c'est l'endroit où le transfert entre les commutateurs de votre réseau prend place.

- Mode VLAN : Affiche le mode VLAN : VLAN basé sur le/la port/balise. Ici, vous pouvez aussi revenir au mode de VLAN basé sur le port.
  - **Add tag** signifie que le paquet sortant du port sélectionné sera inséré avec une balise 802.1Q tag. Utilisez ce paramètre pour les ports de liaisons montantes et descendantes dans votre réseau balisé VLAN.
  - **Don't care** signifie que le paquet sortant du port sélectionné conserve le paquet original reçu au port source. Ceci est le paramètre par défaut lorsque vous la configuration VLAN. Il est recommandé de changer l'option en **Add** ou **Remove Tag**.
  - **Remove tag** signifie que la balise 802.1Q du paquet sortant du port sélectionné ne sera pas envoyée. Utilisez ce paramètre pour la connexion réseau de vos PC. Seulement les paquets du groupe VLAN dont le port est membre seront envoyés.

5.2.2. Membre VLAN

Les ports doivent être faits membres des groupes VLAN. Ceci est pour le mode VLAN basé sur la balise et sur le port. L'écran ici est différente selon le Tag Based ou Port Based Mode.

Membre VLAN dans le mode basé sur le port

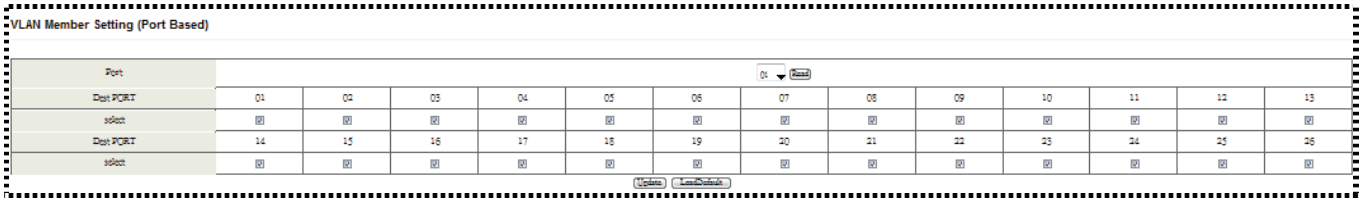


Figure 24 – Groupe les ports pour le mode VLAN base sur le port

Dans le mode Port Based vous voyez une matrice de vos ports. Sélectionnez simplement le port que vous voulez configurer au haut de l’écran, cliquez sur **Read** et ensuite sélectionnez ou désélectionnez les ports qui sont sur le même groupe VLAN. Dans ce mode de configuration, vous n’avez pas besoin de vous préoccuper de définir les groupes VLAN and les ID VLAN.

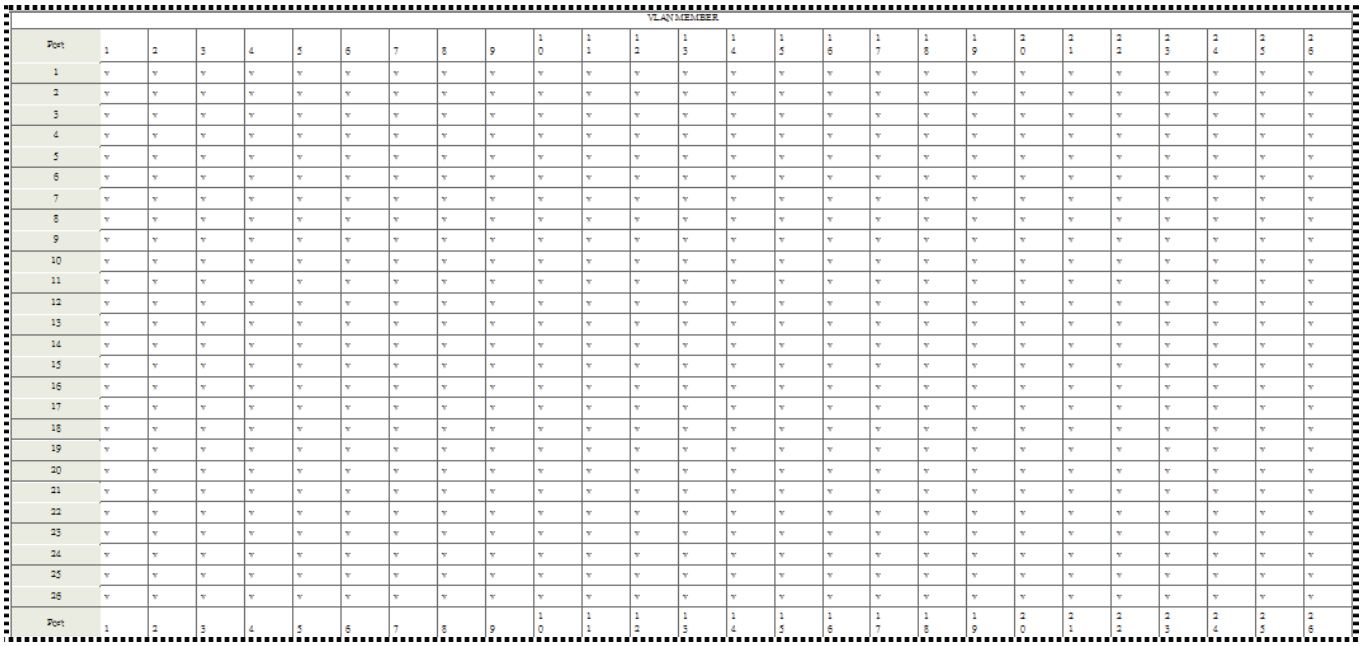
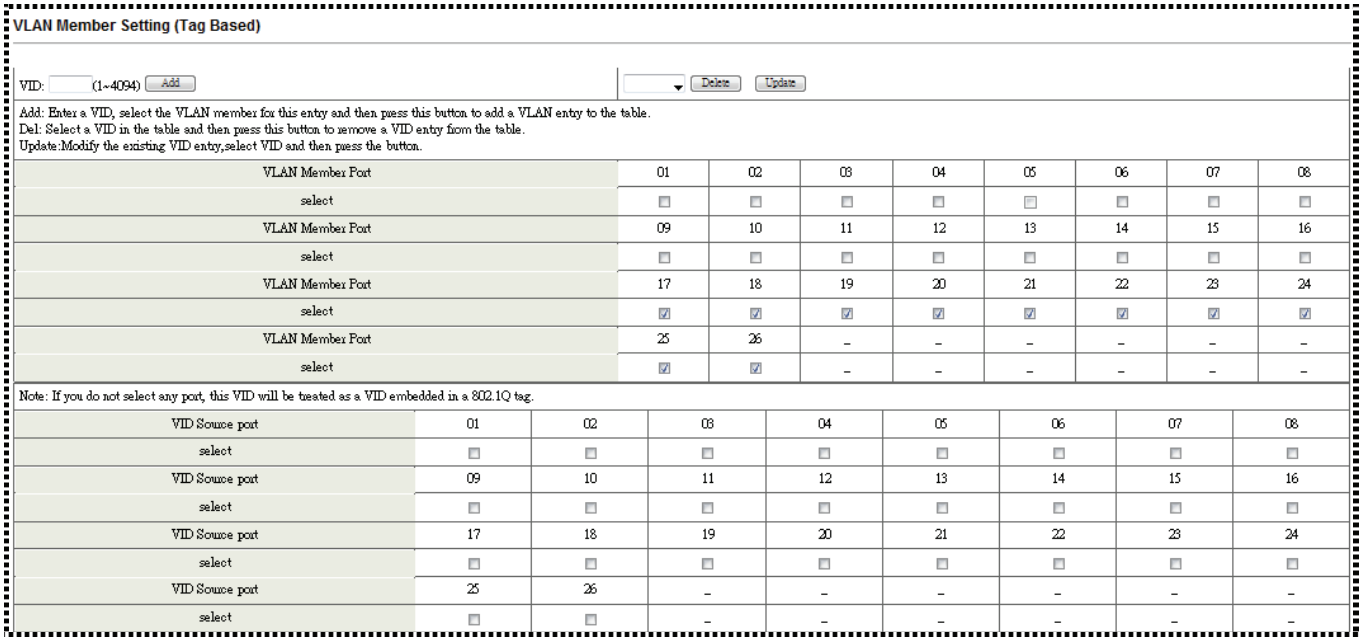


Figure 25 – Un résumé des groupes VLAN

Membre VLAN dans le mode base sur la balise

Dans le mode Tag Based, vous devez définir et configurer vos groupes VLAN. Pour assurer une transition en douceur, les ID (nombres) VLAN doivent être les mêmes que dans le reste du réseau.

Ajouter des groupes VLAN (identifiés à travers votre réseau par des nombres uniques et constants). Commencez avec des ID de 100 et plus. Gardez à l’esprit que certains commutateurs utilisent « 1 » comme nombre par défaut, tandis que d’autres utilisent “4095” ou “4096” par défaut. Commencer avec 100 vous donne assez d’espace et moins de problèmes de compatibilité.



VLAN Member Setting (Tag Based)

VID: (1~4094) Add | Delete | Update

Add: Enter a VID, select the VLAN member for this entry and then press this button to add a VLAN entry to the table.
Del: Select a VID in the table and then press this button to remove a VID entry from the table.
Update:Modify the existing VID entry,select VID and then press the button.

VLAN Member Port	01	02	03	04	05	06	07	08
select	☐	☐	☐	☐	☐	☐	☐	☐
VLAN Member Port	09	10	11	12	13	14	15	16
select	☐	☐	☐	☐	☐	☐	☐	☐
VLAN Member Port	17	18	19	20	21	22	23	24
select	☑	☑	☑	☑	☑	☑	☑	☑
VLAN Member Port	25	26	_	_	_	_	_	_
select	☑	☑	_	_	_	_	_	_

Note: If you do not select any port, this VID will be treated as a VID embedded in a 802.1Q tag.

VID Source port	01	02	03	04	05	06	07	08
select	☐	☐	☐	☐	☐	☐	☐	☐
VID Source port	09	10	11	12	13	14	15	16
select	☐	☐	☐	☐	☐	☐	☐	☐
VID Source port	17	18	19	20	21	22	23	24
select	☐	☐	☐	☐	☐	☐	☐	☐
VID Source port	25	26	_	_	_	_	_	_
select	☐	☐	_	_	_	_	_	_

Figure 26 – Paramètres de balise

Entrez 100 dans le champ à droite du Réglage VID puis sélectionnez ou désélectionnez les ports qui sont membres de ce groupe. Gardez à l'esprit que les liaisons montantes et descendantes des ports doivent contenir des membres de chaque groupe existant. Lorsque les ports sont assignés, cliquez sur **Add**. Le nouveau groupe, avec sa configuration, est affiché au bas de l'écran.

Avec le réglage PVID, définissez VLAN auquel appartient le groupe le trafic entrant. Par exemple, le port 1 est un membre des groupes 100 et 101. Un simple PC est connecté au port 1. Si ce PC est en train d'envoyer des données, avec PVID, définissez si les données sont pour les groupes 100 ou 101.

Un résumé des VLAN peuvent être vus comme affichés dans l'écran ci-dessous.

Port VID Map.								
Port	01	02	03	04	05	06	07	08
VID	—	—	—	—	—	—	—	—
Port	09	10	11	12	13	14	15	16
VID	—	—	—	—	—	—	—	—
Port	17	18	19	20	21	22	23	24
VID	—	—	—	—	—	—	—	—
Port	25	26	_	_	_	_	_	_
VID	—	—	_	_	_	_	_	_

VLAN MEMBER																										
VID \ Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figure 27 – Les ports et leurs ID VLAN

5.3. Configuration de multi à 1

Le VLAN Multi à 1 est utilisé est utilisé dans le côté CPE du « *Ethernet-to-the-Home*. » Lorsque les paramètres du membre VLAN sont mis à jour, le paramètre multi à 1 sera annulé. La désactivation du port l’exclut de cette action. Tous les ports exclus dans ce cadre sont traités comme un même groupe VLAN. Dans un réseau VLAN basé sur la balise normal, cette option de configuration n'est pas
nécessaire.

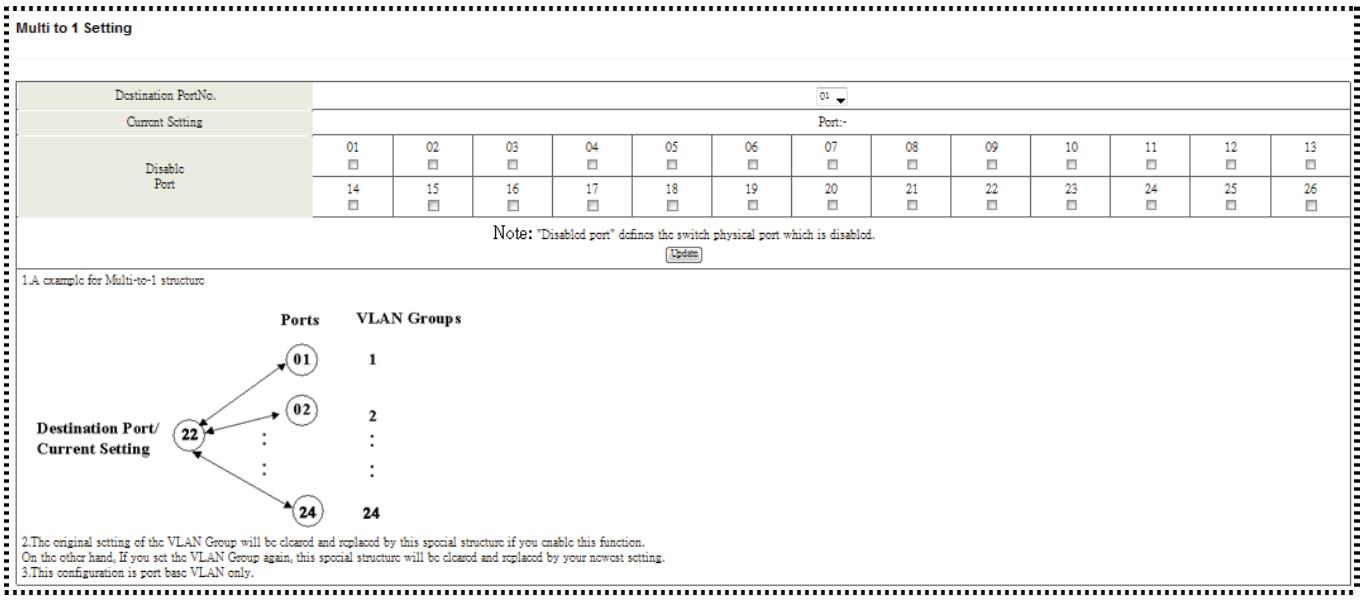

Multi to 1 Setting
Destination PortNo.
Current Setting
Port:-
Disable Port
01 02 03 04 05 06 07 08 09 10 11 12 13
14 15 16 17 18 19 20 21 22 23 24 25 26
Note: "Disabled port" defines the switch physical port which is disabled.
Update
1.A example for Multi-to-1 structure
Ports
VLAN Groups
Destination Port/ Current Setting
22
01
02
24
1
2
24
2.The original setting of the VLAN Group will be cleared and replaced by this special structure if you enable this function.
On the other hand, If you set the VLAN Group again, this special structure will be cleared and replaced by your newest setting.
3.This configuration is port base VLAN only.

Figure 28 – Écran de configuration multi à 1

6. COMPTEUR PAR PORT

Compteur du port

Pour accéder aux statistiques du port, cliquez sur le lien Port Counter dans le panneau de navigation de l'interface web. Cette page fournit des statistiques sur chaque port. Les chiffres sont groupés est quatre catégories : **Receive Packet & Transmit Packet/ Transmit & Collision / Receive Packet & Drop /Receive & CRC error.** Sélectionnez la catégorie dans la liste déroulante **Counter Mode Selection**. Une fois que vous avez changé la catégorie du compteur, le compteur sera effacé automatiquement.

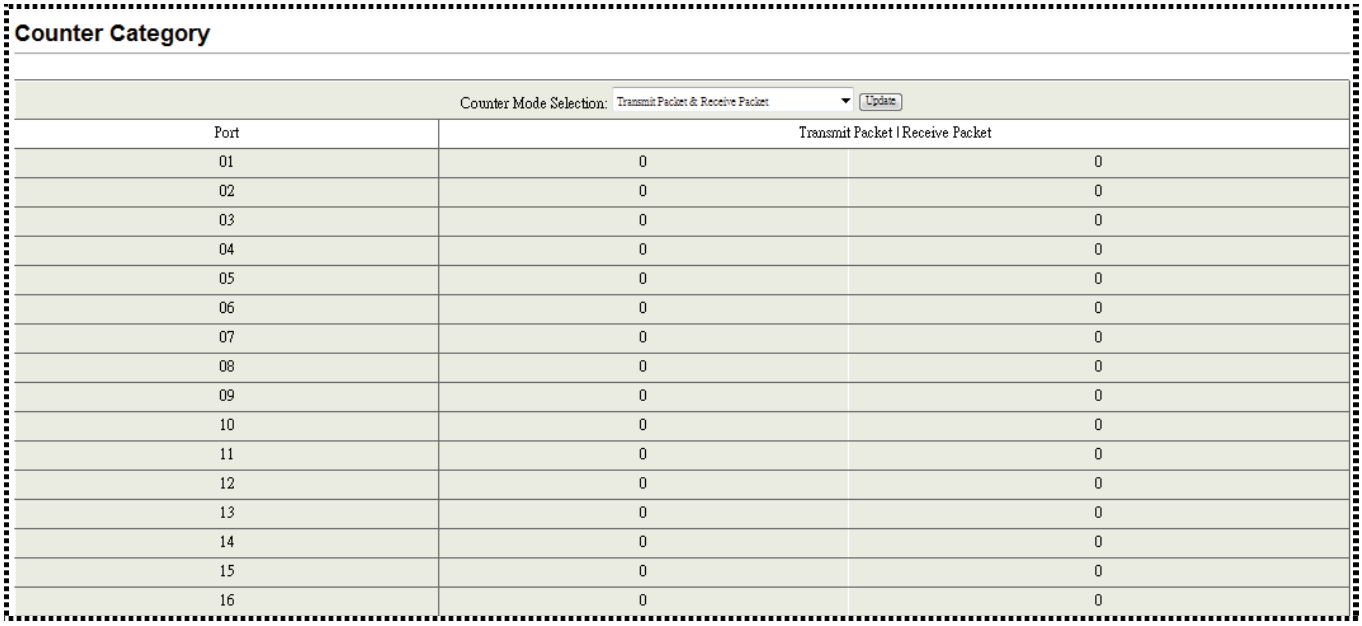


Figure 29 – L'écran de « transmission et de réception des paquets » du compteur par port

- Transmit packet & Receive packet: Le décompte du paquet reçu (excluant les paquets incorrects) et du paquet transmit.
- Collision Count & Transmit packet: Les paquets sortants du commutateur et des collisions.
- Drop packet & Receive packet: Le nombre de paquets valides reçus et le nombre de paquets rejetés.
- CRC packet & Receive packet: Les paquets reçus correct et les erreurs reçues CRC.
- Clear: Cliquer sur **Clear** effacera tous les compteurs.
- Refresh: Cliquer **Refresh** fera la mise à jour des compteurs pour tous les ports.

7. PARAMÈTRE QoS

7.1. À propos de QoS

Ici, vous pouvez configurer le mode de priorité de politique QoS et la configuration CoS (Classe du service). La qualité du service (QoS) est une fonctionnalité avancée du trafic des priorités qui vous permet d'établir un contrôle sur le trafic réseau. La QoS vous permet d'assigner différentes qualités de service réseau pour différents types de trafic, tels que le multimédia, vidéo, protocole spécifique, moment critique et le trafic de fichiers de sauvegarde. La CoS se réfère à des ensembles de fonctionnalités ou des groupes de services qui sont attribués aux utilisateurs en fonction de la politique de l'entreprise. Si un ensemble de fonctionnalités y compris la priorité de transmission, alors CoS est implanté dans les fonctions QoS dans les routeurs et les commutateurs du réseau. Dans un réseau d'entreprise, la classe de service (CoS) différencie le trafic de haute priorité de celui de moindre priorité. Des balises peuvent être ajoutées aux paquets pour identifier ces classes mais ils ne garantissent pas la livraison de même que la qualité du service (QoS) qui sont mises en œuvre dans les périphériques réseau.

La QoS réduit les limitations, les délais, la perte et l’instabilité de la bande passante. Elle fournit également une fiabilité accrue pour la livraison de vos données et vous permet de hiérarchiser certaines applications sur votre réseau. Vous pouvez définir exactement comment vous voulez que le commutateur traite certaines applications et types de trafic.

Vous pouvez utiliser la QoS dans votre système pour :

- Contrôle une large variété de trafic réseau en :
- Classant le trafic en se basant sur les attributs du paquet.
- Assignant les priorités du trafic (par exemple, pour régler le niveau de priorité plus haut des applications qui sont sensibles au temps ou aux affaires).
- Appliquant une politique de sécurité à travers le filtrage du trafic.
- Pourvoyant un débit prévisible pour les applications multimédia comme la vidéo conférence ou l’IP du doublage en minimisant les délais et l’instabilité.
- Améliorant la performance des types spécifiques de trafic et préserver cette performance avec l’augmentation du trafic.
- Réduisant le besoin d’ajouter constamment de la bande passante au réseau.
- Faisant la gestion de la congestion du réseau.

7.2. Configurer la QoS

Pour accéder aux options de configuration de la QoS, cliquez sur le lien ***QoS Settings*** dans le panneau de navigation de

l'interface web.

7.2.1. Mode de priorité

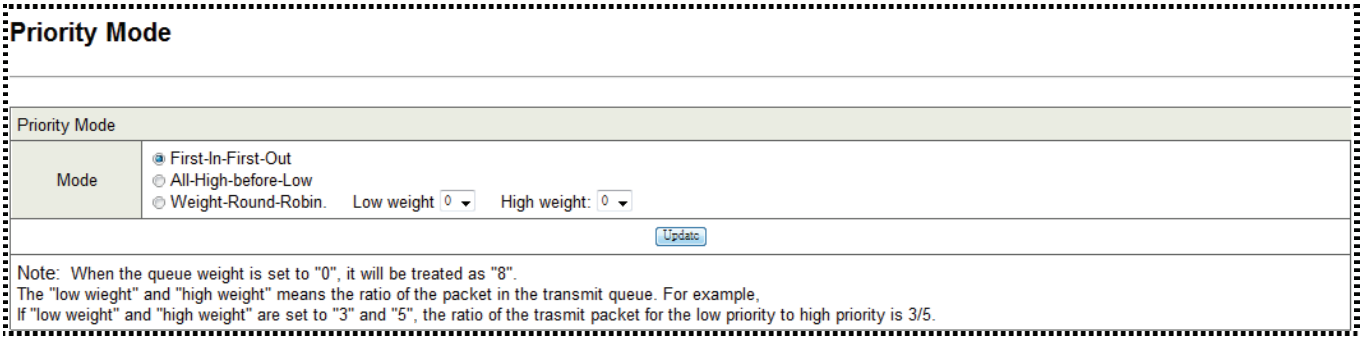

Priority Mode
Priority Mode
Mode
First-In-First-Out
All-High-before-Low
Weight-Round-Robin.
Low weight 0
High weight: 0
Update
Note: When the queue weight is set to "0", it will be treated as "8".
The "low wieght" and "high weight" means the ratio of the packet in the transmit queue. For example,
If "low weight" and "high weight" are set to "3" and "5", the ratio of the trasmit packet for the low priority to high priority is 3/5.

Figure 30 – Sélectionner différents modes

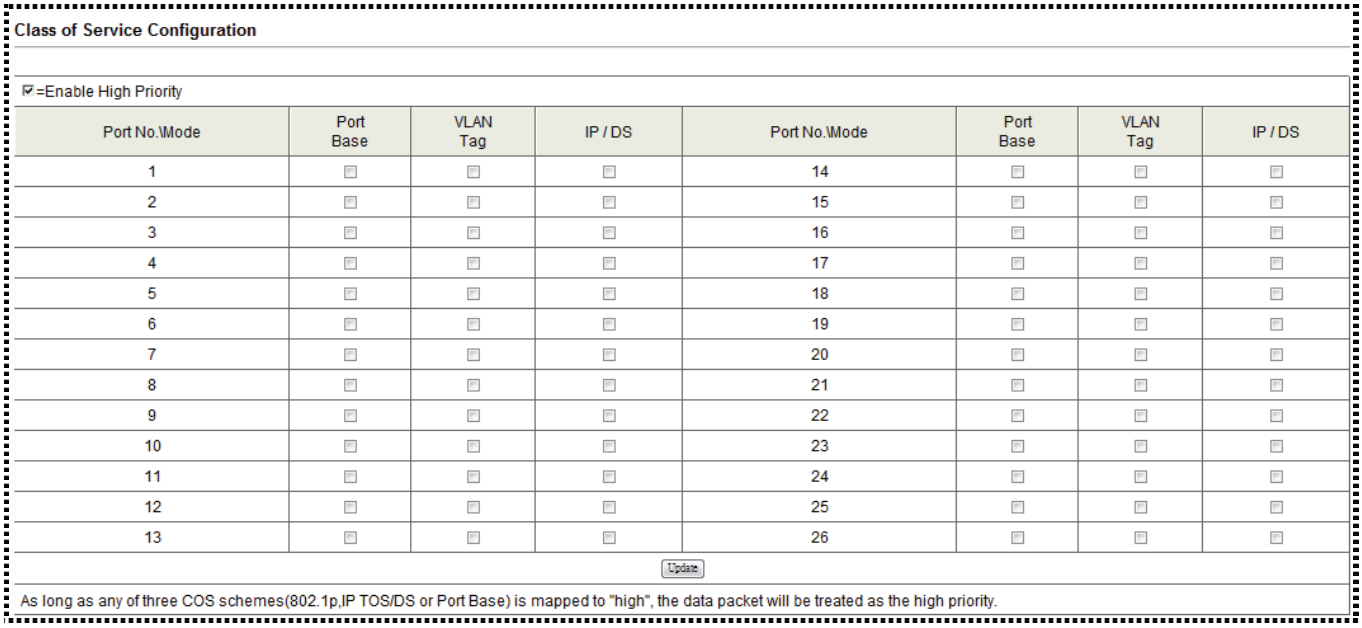
Il y a trois différents modes de priorité disponibles pour spécifier la priorité des paquets en services :

- First-In-First-Out: Les paquets sont placés dans une queue et ils sont desservis dans l'ordre qu'ils ont été reçus.
- All-high-before-low (Strict priority): Tous les paquets seront assignés à soit une queue de niveau de priorité supérieur (Queue 2), soit à une queue de priorité inférieur (Queue 1). Le paquet sur la queue de priorité inférieure ne sera pas envoyé jusqu'à ce que la queue de priorité supérieure soit vide.
- WRR mode: Il y a 4 queues de priorité pour le mode « *Weighted-and-round-robin* » (WRR). Lorsque ce mode est sélectionné, le trafic sera envoyé en fonction du nombre réglé dans chaque queue.

Cliquez sur **Update** pour enregistrer vos modifications.

7.2.2. Port, 802.1p, basé sur IP/DS

Notez que la vérification de la base du port, balise ou IP / DS VLAN fera que le port vérifié sera traité en tant que priorité élevée. Cliquez sur **Update** pour enregistrer vos modifications.



Class of Service Configuration

☑=Enable High Priority

Port No.\Mode	Port Base	VLAN Tag	IP / DS	Port No.\Mode	Port Base	VLAN Tag	IP / DS
1	☐	☐	☐	14	☐	☐	☐
2	☐	☐	☐	15	☐	☐	☐
3	☐	☐	☐	16	☐	☐	☐
4	☐	☐	☐	17	☐	☐	☐
5	☐	☐	☐	18	☐	☐	☐
6	☐	☐	☐	19	☐	☐	☐
7	☐	☐	☐	20	☐	☐	☐
8	☐	☐	☐	21	☐	☐	☐
9	☐	☐	☐	22	☐	☐	☐
10	☐	☐	☐	23	☐	☐	☐
11	☐	☐	☐	24	☐	☐	☐
12	☐	☐	☐	25	☐	☐	☐
13	☐	☐	☐	26	☐	☐	☐

Update

As long as any of three COS schemes(802.1p,IP TOS/DS or Port Base) is mapped to "high", the data packet will be treated as the high priority.

Figure 31 – Choisissez une classe de service

8. SÉCURITÉ

Pour accéder aux options de sécurité, cliquez sur le lien ***Security*** dans le panneau de navigation de l'interface web.

8.1. Contrainte d'adresse MAC

Configurer une adresse MAC permet aux interfaces d'être identifiées uniquement sur votre réseau.

MAC Address Binding

Port No.	MAC Address
1	: : : : : : : : : : : : : : : : : : Read
Select Port 01 Binding Disable Update	

Note: If you enable the MAC address binding function, the address leaning function will be disabled automatically.

Figure 32 – Régler les adresses MAC pour les ports

Port No.	Binding Status	Port No.	Binding Status
1	Disable	14	Disable
2	Disable	15	Disable
3	Disable	16	Disable
4	Disable	17	Disable
5	Disable	18	Disable
6	Disable	19	Disable
7	Disable	20	Disable
8	Disable	21	Disable
9	Disable	22	Disable
10	Disable	23	Disable
11	Disable	24	Disable
12	Disable	25	Disable
13	Disable	26	Disable

Note: The MAC address of current management connection is 00:26:6c:48:af:57 at port 20.

- Port No: Affiche le numéro du port qui est assigné aux adresses MAC.
- MAC Address: Assigner jusqu'à 3 adresses MAC au port.
- Read: Cliquez sur le bouton lire pour afficher les adresses MAC reliées à un port spécifique ou modifier les adresses MAC.
- Select Port: Utiliser le menu déroulant pour choisir un numéro de port à configurer.

- Binding: Sélectionnez ***Enable*** ou ***Disable*** pour la fonction de liaison.

  Cliquez sur **Update** pour enregistrer vos modifications.

8.2. Filtre TCP/UDP

Filtre différents types de connexions vers le réseau sur cette page.

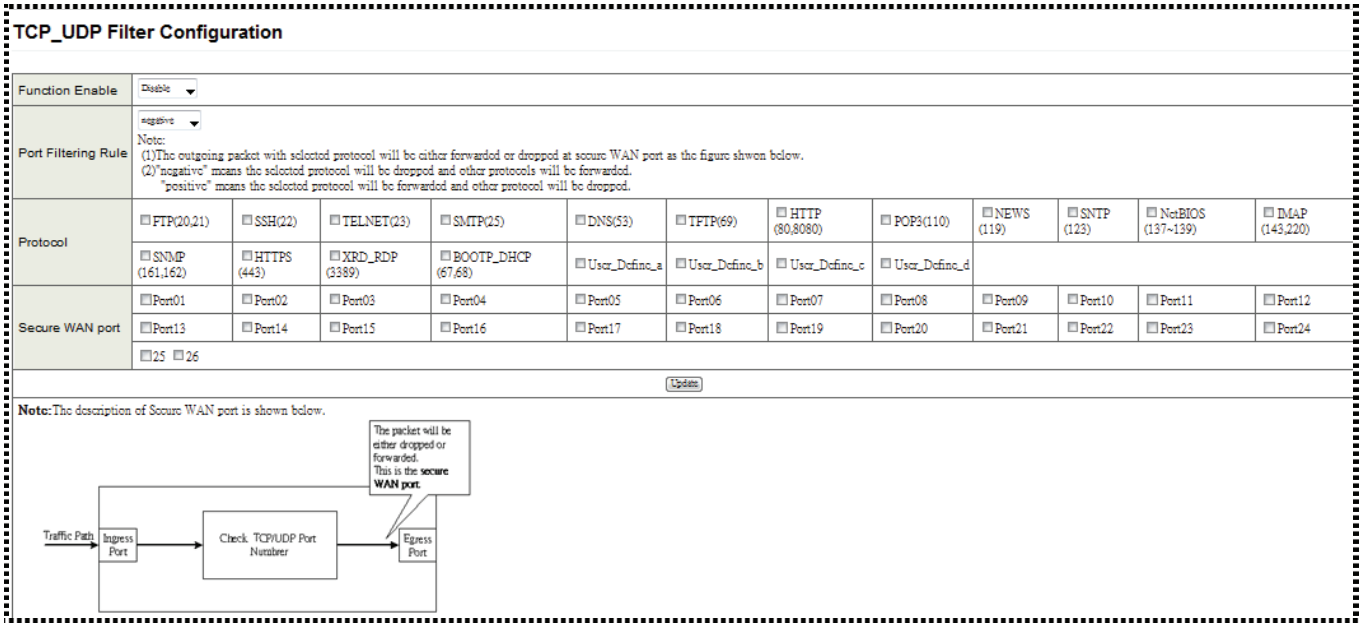


Figure 33 – Filtrer les connexions entrantes et sortantes

- Function Enable: ***Enable*** ou ***Disable*** le filtrage.
- Port Filtering Rule: Pour permettre le renvoi (ne filtre pas), sélectionnez ***négative*** dans le menu déroulant et dans la section protocole, sélectionnez les ports à renvoyer. Pour empêcher le renvoi (filtrer), sélectionnez ***positive*** dans le menu déroulant et dans la section protocole, sélectionnez les ports à filtrer.
- Protocol: Cochez les protocoles à filtrer/renvoyer.
- Secure WAN port: Sélectionnez le port dans lequel le trafic WAN sera envoyé.

  Cliquez sur **Update** pour enregistrer vos modifications.

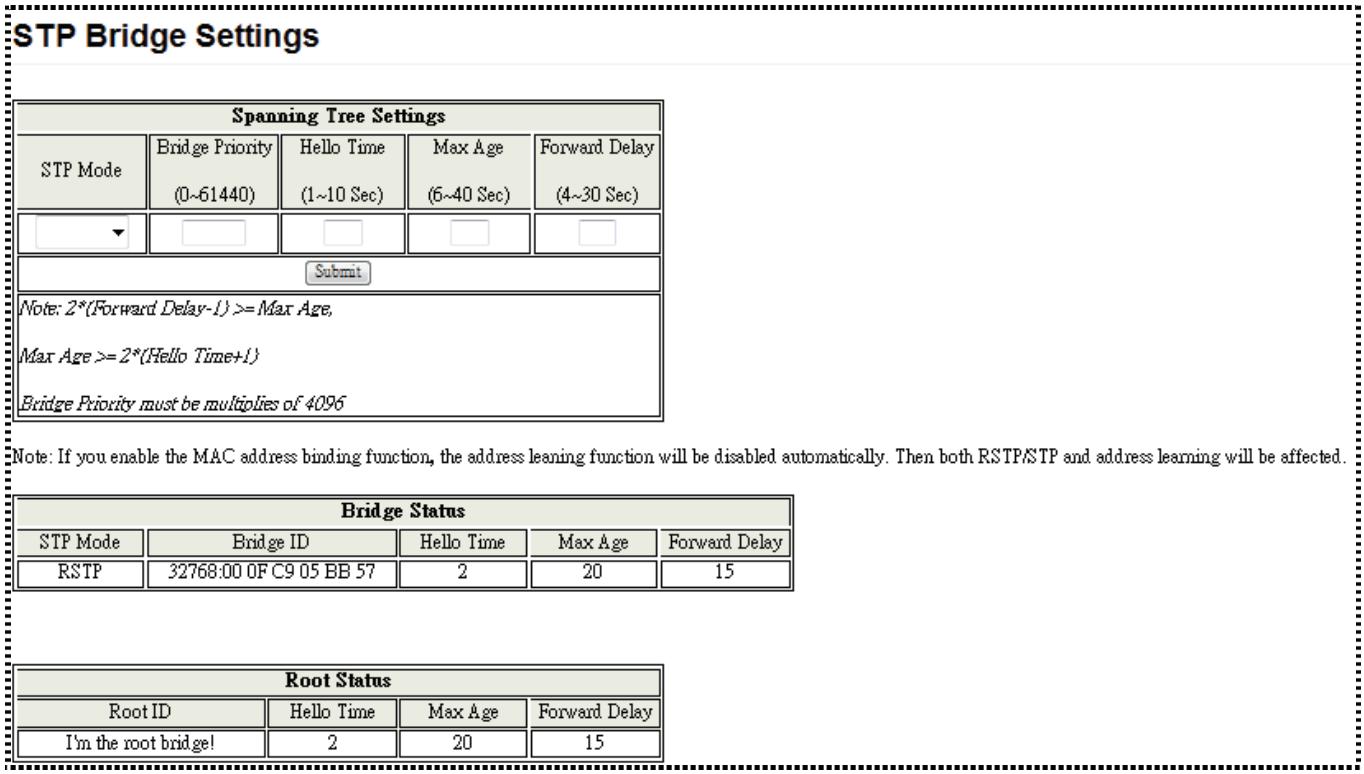
9. « SPANNING TREE PROTOCOL »

Le « *spanning tree protocol* » peut être utilisé pour détecter et désactiver les boucles réseau et fournir des liaisons de sauvegarde entre les commutateurs, les ponts ou les routeurs. Cela permet au commutateur d'interagir avec d'autres dispositifs de pontage dans votre réseau afin de garantir qu'une seule route existe entre deux stations du réseau et de fournir des liaisons de sauvegarde qui prennent automatiquement le relais si le lien principal tombe en panne.

Le protocole permet le blocage des liens entre les commutateurs qui forment des boucles dans le réseau. Lorsque des liens multiples entre les commutateurs sont détectés, un lien primaire est établi. Les liens dupliqués sont ne peuvent être utilisés et deviennent des liens en attente. Le protocole permet aux liaisons doubles d’être utilisées dans le cas où la liaison primaire serait en panne. Une fois que le *protocole Spanning Tree* est configuré et activé, les liens primaires sont établis et les liens dupliqués sont automatiquement bloqués. La réactivation des liens bloqués (au moment de la défaillance de la liaison principale) est également réalisée automatiquement et sans intervention de l'opérateur.

Pour accéder les options du *Spanning Tree*, cliquez sur le lien ***Spanning Tree*** dans le panneau de navigation de l’interface web.

9.1. Paramètres du pont STP



- Bridge Priority: Ce paramètre configure la priorité *spanning tree* globalement pour ce commutateur. Le dispositif avec la priorité la plus haute dévient le dispositif source STP. Cependant, si tous les dispositifs ont la même priorité, le dispositif avec l'adresse MAC la plus basse deviendra alors le dispositif source. Un nombre sélectionné devrait être entre 0 et 61440 en paliers de 4096.
- Hello Time: L'intervalle (en secondes) à l'intérieur duquel le dispositif source transmet un message de configuration (cadre BPDU). Sélectionnez un nombre entre ***1*** et ***10*** (par défaut, c'est le ***2***).
- Max Age – Le temps maximal (en secondes) qu'un dispositif peut attendre sans recevoir de message de configuration avant de tenter de se reconfigurer. Ceci signifie également la durée maximale de vie d'un cadre BPDU. Sélectionnez un nombre entre ***6*** et ***40*** (par défaut, c'est le ***20***).

Forward Delay: Le temps maximal (en secondes) que le dispositif source attendra avant de changer d'état (par exemple, rejeter pour apprendre à renvoyer). Choisissez un nombre de 4 à 30 (par défaut, c'est le 15).

Cliquez sur **Submit** pour enregistrer vos modifications.

9.2. Paramètres du port STP

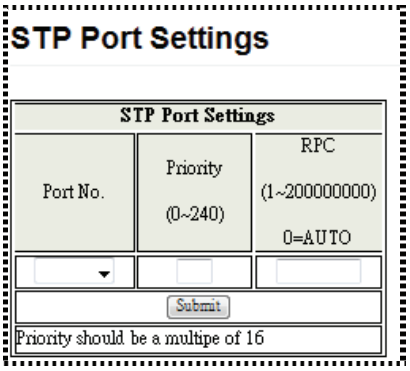


Figure 34 – Paramètres par port

- Port No: L'ID du port. Il ne peut pas être changé. Les agrégations font référence à tout groupe de tronc configuré.
- Root Path Cost: Ce paramètre est utilisé par le STP pour déterminer le meilleur chemin entre les dispositifs. De ce fait, les valeurs les plus basses devraient être assignées aux ports attachés à un media plus rapide et les valeurs les plus hautes devraient être assignées à des ports avec des media plus lents. Configurez le coût du chemin RSTP sur le port entre ***0*** et ***200000000***. ***0*** Indique un coût de chemin calculé automatiquement.
- State: affiche si un port est désigné source ou port bloqué.
- Status: Affiche le statut de la transmission du port, par exemple, en renvoi, désactivé, etc.
- Cliquez sur **Update** pour enregistrer vos modifications.

9.3. Paramètres de détection du bouclage

Cette fonction détecte la présence du trafic réseau qui est redirigé vers sa source. Le statut de tous les ports est donné.

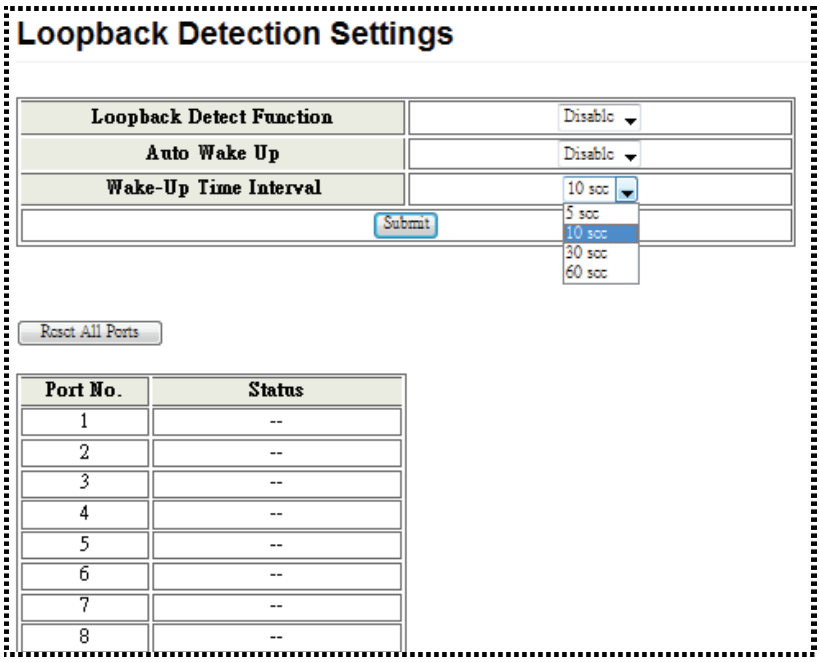


Figure 35 – Écran des paramètres de détection du bouclage

- Loopback Detect Function: Choisissez si vous allez ***Enable*** ou ***Disable*** cette fonction.
- Auto Wake Up: Détermine si le contrôleur est réglé de façon à se réveiller ou non.
- Wake-Up Time Interval: Spécifier la duration dans le menu déroulant.

Cliquez sur **Update** pour enregistrer vos modifications.

10. GROUPAGE DE PORTS (« TRUNKING »)

Le tronc de ports permet à de multiples liens d’être regroupés et d'agir comme une seule liaison physique mais avec un plus grand débit. Ça assure l'équilibrage de charge et la redondance des liens dans un réseau commuté. En tant que tel, le lien n'a pas une bande passante inhérente totale égale à la somme de ses liens physiques. La circulation dans un tronc est distribuée à travers une liaison individuelle à l'intérieur du tronc déterminé par un algorithme de hachage. L'algorithme de hachage applique automatiquement l'équilibrage de charge pour les ports dans le tronc. Une panne du port dans le faisceau fait que le trafic sur le réseau doit être redirigé vers les ports restants. L'équilibrage de charge est mis à jour chaque fois qu'un lien dans un tronc tombe en panne ou est remis en service. Ce commutateur peut utiliser l’ID du port, l’adresse MAC source, l’adresse MAC de destination ou une combinaison de l’adresse source MAC et de l’adresse MAC de destination comme facteur le choix de cet algorithme. Le patron de trafic sur le réseau doit être examiné attentivement avant de l'appliquer. Quand un bon algorithme de hachage est utilisé, la charge du trafic réseau sera équilibrée et le trafic lui-même sera transmis à travers n'importe quel lien dans le tronc.

Pour accéder aux options de groupage de ports, cliquez sur le lien ***Trunking*** dans le panneau de navigation de l’interface web.

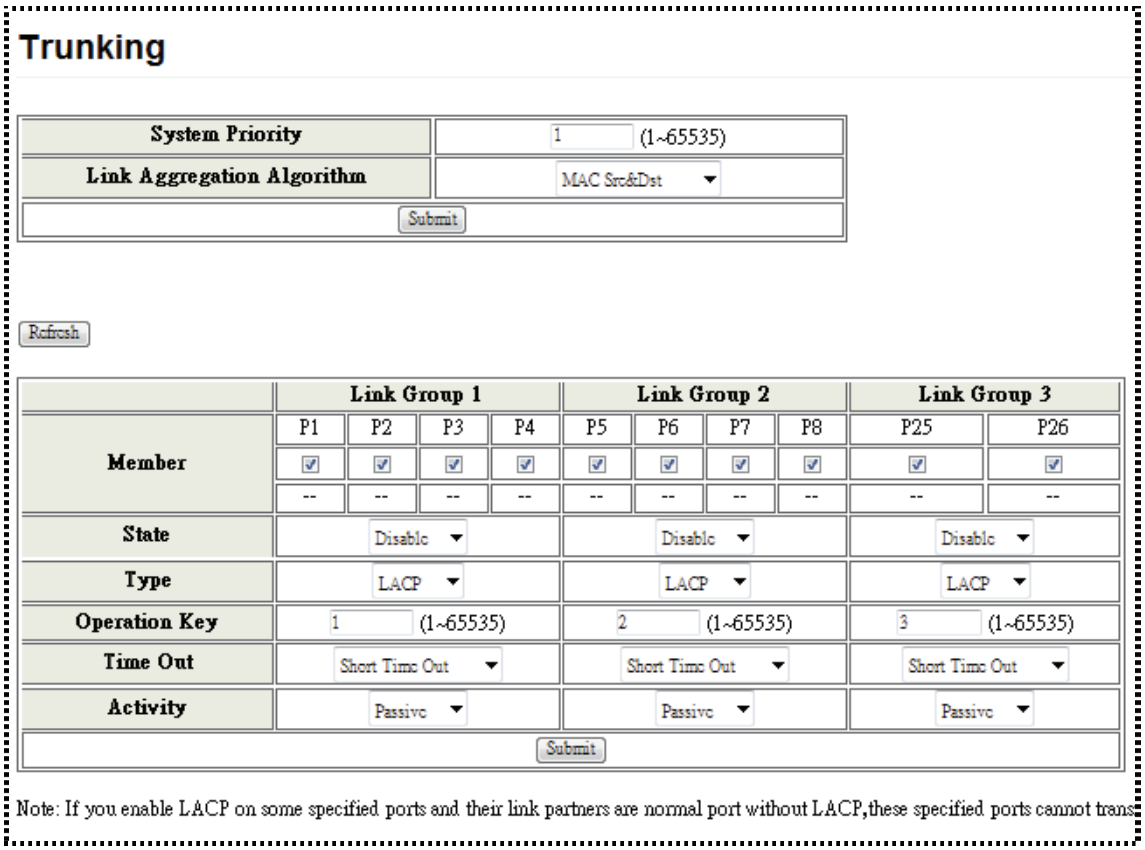


Figure 36 – Écran de groupage

Ce commutateur géré supporte deux groupes de tronc. Chaque tronc consiste en 2 à 4 ports.

- System Priority: Spécifier une priorité entre ***1*** et ***65535***.
- Link Aggregation Algorithm: Utiliser soit ***Port ID***, ***Source MAC Address***, ***Destination MAC Address*** ou ***MAC Src&Dst*** (Source et destination).

Cliquez sur **Submit**

- Member: Groupez les liens en cochant chacune de leurs boîtes. On peut faire jusqu'à trois liens.
- State: ***Enable*** ou ***Disable*** groupage.
- Type: Choisir le type de groupage.
- Operation Key: Spécifier un nombre de ***1*** à ***65535***.
- Time Out: Choisir entre les durations affichées dans le menu déroulant.
- Activity: Sélectionner un mode dans le menu déroulant.

Cliquez sur **Update** pour enregistrer vos modifications.

11. SAUVEGARDE / RESTAURATION

Pour accéder aux options de sauvegarde et de restauration, cliquez sur le lien ***Backup/Recovery*** dans le panneau de navigation de l’interface web.

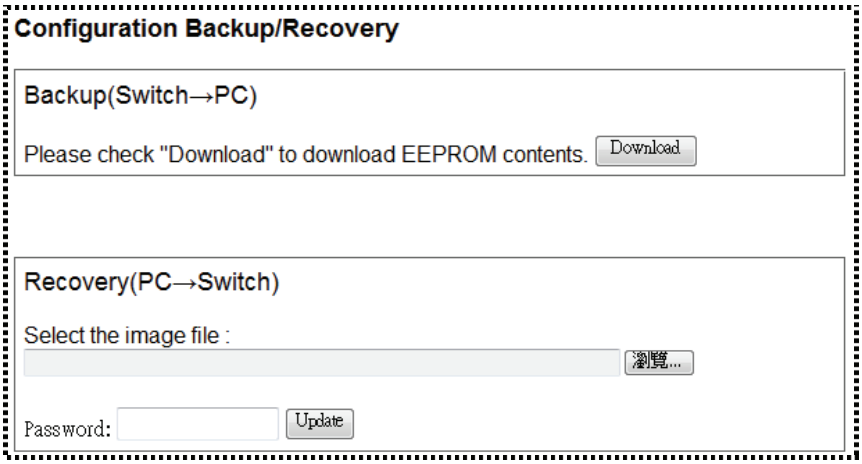


Figure 37 – Options de sauvegarde et de restauration

Cette fonction fournit à l'utilisateur une méthode pour sauvegarder / récupérer la configuration du commutateur. Enregistrer un fichier de configuration en cliquant sur Download. Cela permettra de sauver les réglages actuels d’un fichier. Pour récupérer une configuration, tapez son chemin d'accès dans le champ et entrez le mot de passe de l’administrateur. Cliquez sur **Update** pour enregistrer vos modifications.

12. PARAMÈTRES DIVERS

Les paramètres divers peuvent être utilisés pour configurer le temps de vieillissement d'une queue de sortie, une foulée VLAN et une surveillance IGMP.

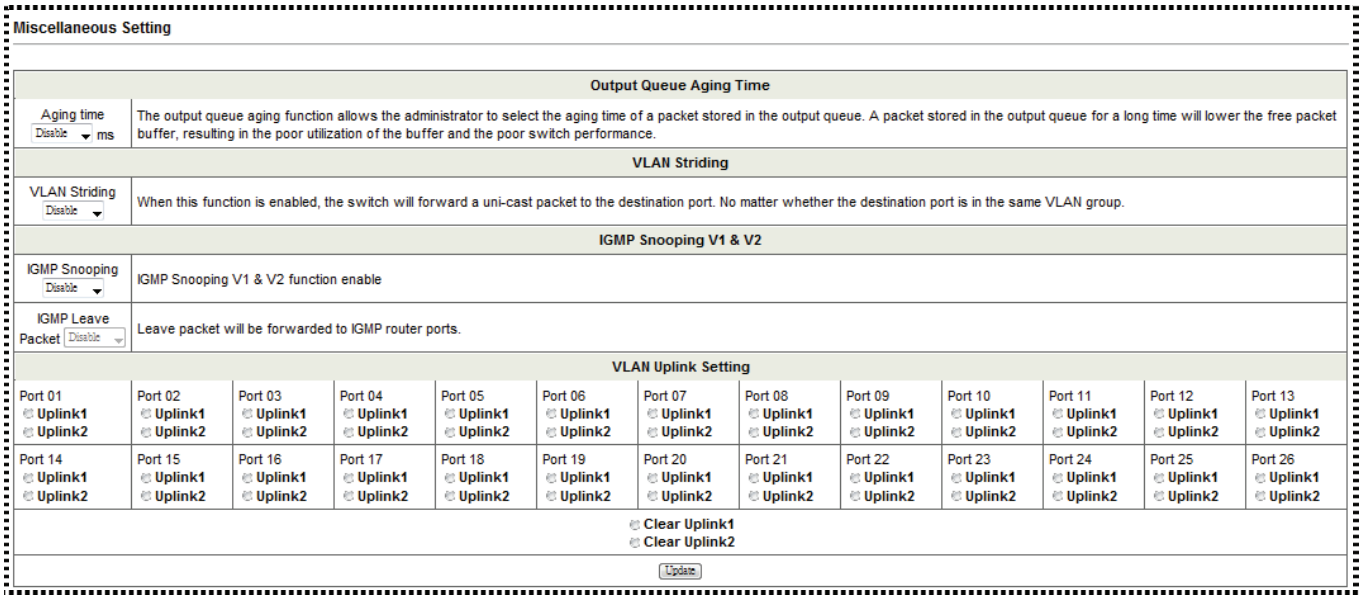

Miscellaneous Setting
Output Queue Aging Time
Aging time
Disable
ms
The output queue aging function allows the administrator to select the aging time of a packet stored in the output queue. A packet stored in the output queue for a long time will lower the free packet buffer, resulting in the poor utilization of the buffer and the poor switch performance.
VLAN Striding
VLAN Striding
Disable
When this function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group.
IGMP Snooping V1 & V2
IGMP Snooping
Disable
IGMP Snooping V1 & V2 function enable
IGMP Leave Packet
Disable
Leave packet will be forwarded to IGMP router ports.
VLAN Uplink Setting
Port 01 Uplink1 Uplink2
Port 02 Uplink1 Uplink2
Port 03 Uplink1 Uplink2
Port 04 Uplink1 Uplink2
Port 05 Uplink1 Uplink2
Port 06 Uplink1 Uplink2
Port 07 Uplink1 Uplink2
Port 08 Uplink1 Uplink2
Port 09 Uplink1 Uplink2
Port 10 Uplink1 Uplink2
Port 11 Uplink1 Uplink2
Port 12 Uplink1 Uplink2
Port 13 Uplink1 Uplink2
Port 14 Uplink1 Uplink2
Port 15 Uplink1 Uplink2
Port 16 Uplink1 Uplink2
Port 17 Uplink1 Uplink2
Port 18 Uplink1 Uplink2
Port 19 Uplink1 Uplink2
Port 20 Uplink1 Uplink2
Port 21 Uplink1 Uplink2
Port 22 Uplink1 Uplink2
Port 23 Uplink1 Uplink2
Port 24 Uplink1 Uplink2
Port 25 Uplink1 Uplink2
Port 26 Uplink1 Uplink2
Clear Uplink1
Clear Uplink2
Update

Figure 38 – Paramètres divers

- Output queue aging: Lorsqu'un paquet est rangé dans un commutateur pour un long moment, il expirera après le temps de vieillissement alloué défini par le protocole et devient un paquet inutilisé. Pour éviter que ces paquets ne gaspillent pas de la bande passante cette option les enlèvera.
- VLAN Striding: En sélectionnant cette fonction, les paquets de monodiffusion sont renvoyés vers le port de destination même si le port de destination est dans le même VLAN.
- IGMP Snooping: Le commutateur fera de la surveillance IGMP de version 1 et de version 2 sans intervention CPU. Le commutateur s'occupe immédiatement des paquets IGMP rapportés et partis.
- IGMP Leave: ***Enable*** ou ***Disable*** le renvoi d'un paquet partit vers les ports routeurs IGMP.

Cliquez sur **Update** pour enregistrer vos modifications.

13. DÉPANNAGE

Ce chapitre contient de l'information pour vous aider à résoudre des problèmes qui peuvent arriver lors de l'utilisation du commutateur.

Le LED *Link* n'est pas allumé

- Solution : Vérifiez la connexion du câble et enlevez le mode duplex du commutateur Ethernet.
-

Certaines stations ne peuvent pas parler à d'autres stations situées sur un autre port

Solution : S'il vous plaît vérifiez les paramètres VLAN, les paramètres du tronc ou le statut du port activé / désactivé.

La performance est mauvaise

Solution : Vérifiez l'état du statut *full duplex* du commutateur Ethernet. Si le commutateur Ethernet est en *full duplex* complet et que le partenaire est réglé en mode *half duplex*, les performances seront médiocres. S'il vous plaît, veuillez également consulter le taux entrant/sortant du port.

Le commutateur ne se connecte pas à un réseau

Solution : Vérifiez la LNK/ACT LED sur le commutateur

Essayez un autre port sur le commutateur

Solution :

- Assurez-vous que le câble est correctement installé
- Assurez-vous que le câble est du bon type
- Coupez l'alimentation. Après un certain temps, remettez l'appareil sous tension

100Base-TX liaison du port est allumé mais le trafic est irrégulier

Solution: Vérifiez que le périphérique connecté n'est pas réglé à full duplex. Certains appareils utilisent un commutateur physique ou un logiciel pour changer de mode duplex. La négociation automatique ne peut pas reconnaître ce type de réglage full-duplex.

L'interrupteur ne s'allume pas

- Solution :
  - Le cordon d'alimentation est soit débranché ou défectueux ; verifiez que le cordon d'alimentation est inséré correctement et remplacer si nécessaire.

- Vérifiez si la source d’alimentation fonctionne en connectant un autre dispositif à la place du commutateur.

Perdu le mot de passe de l’administrateur

Solution : Voir la section Administration de l'information sur la façon de réinitialiser le commutateur et les paramètres par défaut

ANNEXE A : PÉRIPHÉRIQUE RÉSEAU

A.1. Affectation des pins RJ-45

Affectation de la broche 1000Mbps, 1000Base.

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Tableau 3 – Affectation de la pin pour 1000 Mbps, 1000 BaseT

Implantation implicite de la fonction *crossover* dans un câble à paire torsadée ou à un panneau de câblage, tout en n'étant pas expressément interdit, est au-delà du champ d'application de cette norme.

A.2. 10/100Mbps, 10/100Base-TX

Lorsque vous connectez votre commutateur Ethernet 10/100Mbps à un autre commutateur, un pont ou un hub, un câble direct ou croisé est nécessaire. Chaque port du commutateur est en charge de la détection auto-MDI/MDI-X. Cela signifie que vous pouvez connecter directement le commutateur avec n'importe quel autre périphérique Ethernet sans avoir un câble croisé. Le tableau et le diagramme ci-dessous montrent le standard RJ-45 femelle / mâle et l'affectation de chaque broche :

Contact	Interface dépendante au média MDI	Interface-croisée dépendante au média MDI-X
1	Tx + (transmettre)	Rx + (recevoir)
2	Tx - (transmettre)	Rx - (recevoir)
3	Rx + (recevoir)	Tx + (transmettre)
4, 5	Pas utilisé	
6	Rx - (recevoir)	Tx - (transmettre)

7, 8	Pas utilisé

Tableau 4 – Affectation de chaque pin pour 10/100 Mbps, 10/100 BaseTX

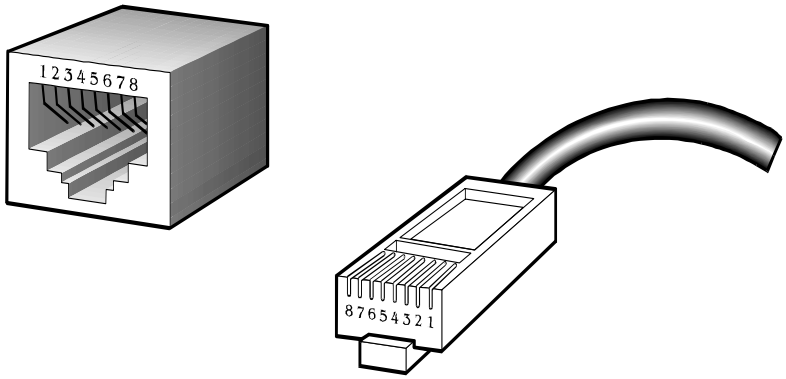


Figure 39 – Port et connecteur RJ-45

Il y a 8 fils sur un câble UTP / STP normal et chaque fil est codé avec une couleur. Le tableau suivant montre l'affectation des pins, la couleur des câbles directs et la connexion du câble croisé :

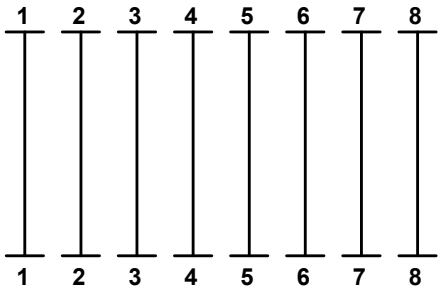
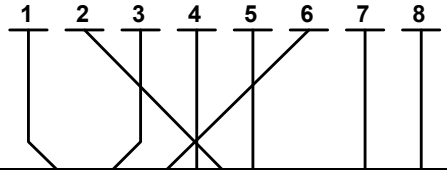
Câble droit		CÔTÉ 1	CÔTÉ 2
	CÔTÉ 1	1 = Blanc / Orange	1 = Blanc / Orange
	CÔTÉ 2	2 = Orange	2 = Orange
		3 = Blanc / Vert	3 = Blanc / Vert
		4 = Bleu	4 = Bleu
		5 = Blanc / Bleu	5 = Blanc / Bleu
		6 = Vert	6 = Vert
		7 = Blanc / Brun	7 = Blanc / Brun
		8 = Brun	8 = Brun

Tableau 5 – Pins de câbles directs

Câble croisé		CÔTÉ 1	CÔTÉ 2
	CÔTÉ 1	1 = Blanc / Orange	1 = Blanc / Vert
		2 = Orange	2 = Vert
		3 = Blanc / Vert	3 = Blanc / Orange
			4 = Bleu

	CÔTÉ 2	4 = Bleu 5 = Blanc / Bleu 6 = Vert 7 = Blanc / Brun 8 = Brun	5 = Blanc / Bleu 6 = Orange 7 = Blanc / Brun 8 = Brun

Tableau 6 – Pins de câbles croisés

S'il vous plaît assurez-vous que les câbles connectés ont la même affectation des pins et des couleurs que l'image ci-dessus avant d’effectuer le déploiement des câbles dans votre réseau.

ANNEXE B: Store-and-Forward

Store-and-Forward est un type de technique de renvoi de paquet. Un commutateur *Store-and-Forward* Ethernet stocke la trame entrante dans une mémoire tampon interne; une vérification d'erreur complète est effectuée avant la transmission afin d'éliminer la présence de paquets erronés. C'est le meilleur choix lorsque l'efficacité et la stabilité du réseau sont une priorité.

Le commutateur balaye l'adresse de destination de l'entête du paquet, recherche dans la table de routage fournies pour le port d'entrée et transmet le paquet, seulement si nécessaire. La transmission rapide rend le commutateur idéal pour connecter les serveurs directement au réseau, augmentant ainsi le débit et la disponibilité. Toutefois, le commutateur est le plus couramment utilisé pour segmenter des concentrateurs existants, qui presque toujours améliore les performances globales. Un commutateur Ethernet peut être facilement configuré dans n'importe quel environnement réseau pour stimuler de manière significative la bande passante en utilisant le câblage conventionnel et des adaptateurs.

En raison de la fonction d'apprentissage du commutateur, l'adresse source et le numéro de port correspondant de chaque paquet entrant et sortant sont stockés dans une table de routage. Cette information est ensuite utilisée pour filtrer les paquets dont l'adresse de destination se trouve sur le même segment que l'adresse source. Cela confines le réseau du trafic réseau à son domaine respectif et réduit la charge globale sur le réseau.

Le commutateur effectue le "Store and forward», donc, aucune erreur de paquet ne survient. Plus fiable, il réduit le taux de ré-émissions. Aucune perte de paquets ne se produira.

ANNEXE C : Aperçu du PoE

IEEE802.3af, aussi appelé alimentation d'équipement terminal de données (DTE) par l'intermédiaire des médias interface dépendante (MDI), est une norme internationale qui définit la transmission de puissance sur Ethernet. 802.3af fournit une puissance de 48V sur le câblage RJ-45. Outre la norme 802.3af, deux types de matériel source sont définis: à *Mid-Span* et *End-Span*.

- **Mid-Span**

  Un dispositif *Mid-Span* est placé entre un commutateur et le périphérique alimenté. Mid-Span exploite les paires de fils inutilisées 4/5 et 7/8 pour acheminer l'électricité. Les quatre autres sont réservées pour la transmission de données.

- **End-Span**

  Un dispositif *End-Span* se connecte directement à un dispositif d'alimentation. Les dispositifs *End-Span* peuvent aussi exploiter les paires de fils 1/2 et 3/6.

C.1. Architecture système AvE (PoE)

La spécification de la technologie AvE (PoE) nécessite généralement deux dispositifs: l'équipement *Source Powered* (PSE) et le périphérique alimenté (PD). Le PSE est soit un *End-Span* ou un mi-portée, tandis que le PD est un terminal AvE (PoE), tel que les téléphones IP, Wireless LAN, etc, L'alimentation peut être livré sur des paires de données ou des paires de rechange de la norme de câblage CAT-5.

C.1.1. Transfert d'alimentation via un câble Ethernet CAT5

Un câble Ethernet CAT5 standard a quatre paires torsadées, mais seulement deux d'entre elles sont utilisées pour les spécifications 10BASE-T et 100BASE-T. La spécification permet deux options pour l'utilisation de ces câbles pour l'alimentation, illustré à la figure 8-1 et Figure 8-2: Les paires de rechange sont utilisées dans ces diagrammes; La Figure 8-1 montre la paire sur les broches 4 et 5 reliées entre elles, formant une alimentation positive et la paire de broches 7 et 8 reliées, formant une alimentation négative. En utilisation réelle, les deux polarités peuvent être utilisées pour le transfert de l'alimentation.

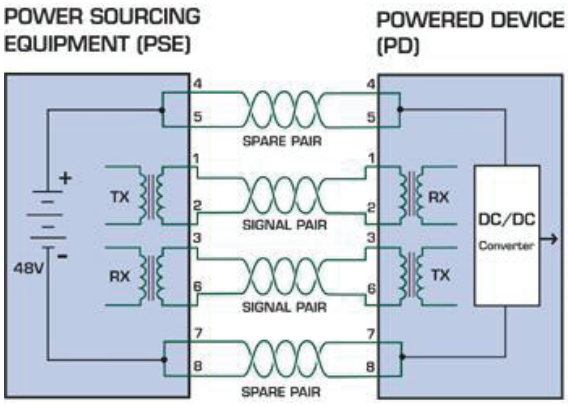


Table 7 - Power supplied over spare pins

Les paires de données sont utilisées. Comme les paires Ethernet sont des transformateurs couplés à chaque extrémité, un courant continu peut être appliquée à la prise centrale du transformateur d'isolement sans perturber le transfert de données. Dans ce mode de fonctionnement, la paire sur les broches 3 et 6 et la paire sur les broches 1 et 2 peuvent être de n'importe quelle polarité.

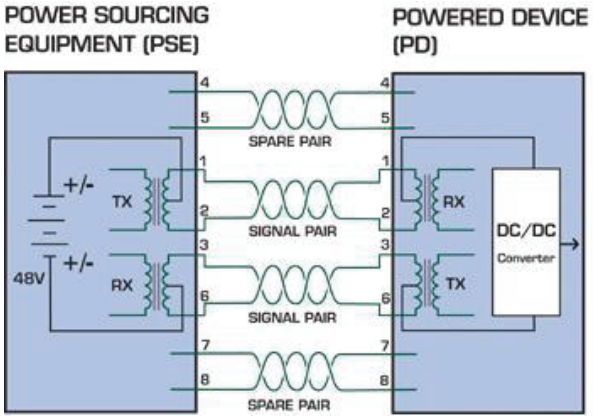


Table 8 - Power supplied over data pins

Références :

- IEEE Std 802.3af-2003
  - (Amendement à IEEE Std 802.3-2002, incluant IEEE Std 802.3ae-2002), 2003 Page(s) :0_1-121
- Papier blanc sur l'alimentation de l'Ethernet (IEEE802.3af)
  - Hhttp://www.poweroverethernet.com/articles.php?article_id=52
- Microsemi /PowerDsine
  - Hhttp://www.microsemi.com/PowerDsine/
- Tech linéaire
  - Hhttp://www.linear.com/

C.2. Processus d'approvisionnement AvE (PoE)

Malgré le fait que l'ajout du support PoE aux périphériques réseau est une opération relativement simple, lisez cette section attentivement et comprenez ce processus avant de tenter d'initialiser un tel réseau afin de minimiser le risque de dommages au matériel non conçu pour la fourniture d'énergie sur le réseau.

Le PSE est un périphérique qui gère le flux de puissance sur un câble Ethernet. Au cours de la période de détection, un petit niveau de tension est induit sur la sortie du port jusqu'à ce qu'un PD soit détecté. Le PSE peut choisir d'effectuer la classification, à estimer la quantité d'énergie devant être consommée par ce PD. Après un démarrage temporisé, le PSE commence à fournir les 48 Volts DC au DP, jusqu'à ce qu'il soit physiquement ou électriquement déconnecté, au cours duquel la tension et le courant seront fermés.

Alors que le PSE est responsable de la synchronisation du processus AvE (PoE), il est celui qui génère les signaux de sondage avant d'utiliser le PD et de surveiller les différents scénarios qui peuvent survenir pendant le fonctionnement. Tout sondage est fait en utilisant l'induction de tension et de mesure du courant de retour.

Étape	Action	Voltage spécifié par 802.3af	Voltage géré par le jeu de puces
Détection	Mesure si l'appareil alimenté à la bonne signature de résistance de 15–33 kΩ	2.7-10.0	1.8–10.0
Classification	Mesure quelle classe de niveau d'alimentation la résistance indique	14.5-20.5	12.5–25.0
Démarrage	Où l'appareil alimenté démarrera	>42	>38
Opération normale	Fournitune alimentation à l'appareil	36-57	25.0–60.0

C.2.1. Détection de ligne

Avant que l'alimentation soit appliquée, pour des raisons de sécurité, un PD valide est connecté à la sortie du PSE en premier. Ce processus est appelé «détection de ligne", et implique que le PSE recherche une signature spécifique de résistance de 25 kOhms. La détection de cette signature indique qu'un PD valide est connecté, et que la fourniture d'énergie à l'appareil peut commencer. La signature de résistance est isolé dans le PD AvE (PoE), à l'écart du reste de circuits du PD, jusqu'à ce la détection soit certifiée.

C.2.2. Classification

Une fois qu'un PD est détectée, le PSE peut éventuellement effectuer une classification pour déterminer la puissance

maximale qu'un PD peut consommer. Le PSE induit 15,5 à 20,5 VDC, limitée à 100 mA, pendant une période de 10 à 75 ms répondu par une certaine consommation de courant par le PD, indiquant sa classe de puissance.

Le PD est attribué à l'un des 5 classes: 0 (classe par défaut) indique que 15,4 watts complètes devront être fournies, 1-3 indiquent les différents niveaux de puissance requis et 4 est réservé pour une utilisation future. Le PD qui ne prend pas en charge la classification se voit attribuer la classe 0. Une attention particulière doit être employé dans la définition de seuils de classe, puisque la classification peut être affectée par les pertes dans les câbles.

Le classement d'un PD en fonction de sa consommation d'énergie contribue idéalement un système AvE (PoE) à optimiser sa distribution de puissance, de sorte que la gestion efficace de l'énergie basée sur les résultats de classification peut réduire les coûts totaux du système.

C.2.3. Démarrage

Une fois la détection de ligne et les étapes de classification optionnels sont terminées, le PSE doit passer de basse tension à sa pleine capacité de tension (44-57 volts) sur un laps de temps minimum (plus de 15 microsecondes). Un démarrage progressif est nécessaire pour éviter une hausse brutale de la tension (pour atteindre les hautes fréquences) qui introduirait du bruit sur les lignes de données. Une fois que la distribution d'énergie est lancée, il est courant d'expérimenter un afflux au port PSE, en raison de la capacité d'entrée du PD. Un PD doit être conçu pour cesser la consommation de l'afflux de courant (de plus de 350 mA) à moins de 50 ms du démarrage de disposition de l'alimentation.

C.2.4. Opération

Lors de l'utilisation normale, le PSE fournit 44-57 VDC, capable de supporter un minimum de puissance de 15.4 watts.

C.2.5. Surcharge de puissance

La norme IEEE 802.3af définit le traitement des conditions de surcharge. Dans le cas d'une surcharge (un PD tirant une puissance plus élevée que les 12,95 watts permis), ou un court-circuit causé par une défaillance dans le câblage ou dans le PD, le PSE doit couper le courant dans les 50 à 75 millisecondes, tout en limitant la fuite durant cette période afin de protéger l'infrastructure de câblage. Une chute de tension immédiate est évitée afin de prévenir une coupure due à des fluctuations aléatoires.

C.3. Scénarios de déconnexion de l’alimentation

La norme IEEE 802.3af exige que les appareils alimentés par câble Ethernet soient débranchés en toute sécurité (par

exemple, l’alimentation doit être arrêtée dans un court laps de temps après la déconnexion d'un PD à partir d'un port actif). Lorsqu’un PD est débranché, il y a un risque qu'il sera remplacé par un dispositif non-PoE prêt si l’alimentation est toujours branchée, pour éviter d'endommager l'appareil et des blessures.

La norme définit deux moyens de déconnexion, la déconnexion DC et la déconnexion AC, qui offrent tous deux les mêmes fonctionnalités – PSE arrête l’alimentation vers un port débranché à l’intérieur de 300 à 400 ms. La limite supérieure est une limite physique de l'homme pour déconnecter et reconnecter un autre PD.

- Déconnection DC

La détection de la déconnexion DC consiste à mesurer le courant. Un PD déconnecté arrête de consommer du courant, ce qui peut être inspecté par l'ESP. Le PSE doit donc couper l'alimentation à moins de 300 à 400 ms de l'arrêt de la circulation du courant. La limite inférieure du temps est importante pour éviter l'arrêt dû à des fluctuations aléatoires.

- Déconnexion AC

Cette méthode est basée sur le fait que lorsqu'un PD valide est connecté à un port, l'impédance en courant alternatif mesurée à ses bornes est sensiblement plus faible que dans le cas d'un port ouvert (déconnecté PD).

La détection de la déconnexion AC implique l'induction de signal alternatif bas en plus du voltage d’opération de 48 VDC. L’amplitude du retour de signal AC est contrôlée par l'ESP à des terminaux portuaires. En fonctionnement normal, l’impédance relativement faible du PD abaisse le signal AC de retour, alors qu’une déconnexion soudaine de cette PD provoquera une hausse du niveau de signal alternatif complet et indiquera la déconnexion PD.

APPENDICE D : GLOSSARY

A

Agrégation

L’agrégation est une méthode où de multiples ports sont utilisés en parallèle pour augmenter la vitesse liaison au-delà des limites d’un seul port et pour augmenter la redondance d’une plus grande disponibilité.

D

DEI

DEI est un acronyme qui signifie abandonner l’indicateur admissible (*Drop Eligible Indicator*). C’est un champ de 1 octet dans la balise VLAN.

DHCP

DHCP est l'acronyme de *Dynamic Host Configuration Protocol*. Il est un protocole utilisé pour attribuer des adresses IP dynamiques aux périphériques d'un réseau.
DHCP est utilisé par les ordinateurs en réseau (clients) pour obtenir des adresses IP et d'autres paramètres tels que la passerelle par défaut, masque de sous réseau, et les adresses IP des serveurs DNS à partir d'un serveur DHCP.
Le serveur DHCP veille à ce que toutes les adresses IP soien uniques, par exemple, aucune adresse IP n'est affectée à un second client tandis que l'assignation du premier client est valide (son bail n'a pas expiré). Par conséquent, la gestion des bassins IP est effectuée par le serveur et non par un administrateur humain du réseau.
L'adressage dynamique simplifie l'administration du réseau, car le logiciel garde une trace des adresses IP plutôt que d'exiger un administrateur pour gérer la tâche. Cela signifie qu'un nouvel ordinateur peut être ajouté à un réseau sans les tracas d'une assignation manuelle d'une adresse IP unique.

Relais DHCP

Le relais DHCP est utilisé pour transmettre et transférer les messages DHCP entre les clients et le serveur quand ils ne sont pas sur le même domaine de même.
L'option DHCP 82 permet à un agent de relais DHCP d'insérer des informations spécifiques dans une requête de paquets

DHCP lors de la transmission des paquets DHCP client à un serveur DHCP et de supprimer les informations spécifiques à partir d'une réponse DHCP lors de la transmission des paquets du serveur DHCP à un client DHCP. Le serveur DHCP peut utiliser cette information pour mettre en œuvre l'adresse IP ou d'autres stratégies d'attribution. Plus précisément, l'option fonctionne établissant deux sous-options: ID Circuit (option 1) et ID à distance (option2). La sous-option de ID Circuit est censée inclure des informations spécifiques du circuit de provenance. La sous-option de ID à distance a été conçue pour transporter des informations relatives à l'hôte distant de fin circuit.
La définition du ID Circuit dans le commutateur est de 4 octets de longueur et le format est "vlan_id" "module_id" "port_no". Le paramètre de «vlan_id" sont les deux premiers octets représentent l'ID de VLAN. Le paramètre de «module_id" est le troisième octet pour l'ID du module (dans le commutateur autonome il toujours égal à 0, dans le commutateur empilable cela signifie ID du commutateur). Le paramètre de «port_no" est le quatrième octet et cela signifie le numéro de port.

Le ID à distance est de 6 octets de long, et la valeur est égale à la *MAC address* de l'agent de relais DHCP.

Surveillance DHCP

La surveillance DHCP est utilisée pour bloquer les intrus sur les ports non fiables du commutateur lorsqu'il tente d'intervenir en injectant un paquet de réponse DHCP bidon à une conversation légitime entre le client et le serveur DHCP.

DNS

DNS est un acronyme pour *Domain Name System*. Il stocke et associe de nombreux types d'information avec les noms de domaine. Plus important encore, le DNS traduit les noms de domaine « humains » et les noms d'hôtes en adresse IP. Par exemple, le nom de domaine www.example.com pourrait se traduire à l'adresse 192.0.0.20.

I

IEEE 802.1X

IEEE 802.1X est une norme IEEE pour le port-*based Network Access Control*. Il fournit une authentification à des appareils connectés à un port LAN, établissant une connexion point-à-point ou empêchant l'accès de ce port si l'authentification échoue. Avec la norme 802.1X, l'accès à tous les ports du commutateur peut être commandé de façon centralisée à partir d'un serveur, ce qui signifie que les utilisateurs autorisés peuvent utiliser les mêmes informations d'identification pour l'authentification à partir de n'importe quel point au sein du réseau.

IGMP

IGMP est un acronyme pour *Internet Protocol Management Group*. Il s'agit d'un protocole de communication utilisé pour

gérer la composition des groupes de protocole Internet de multidiffusion. IGMP est utilisé par les hôtes IP et routeurs adjacents de multidiffusion pour établir les adhésions des groupes de multidiffusion. Il est une partie intégrante de la spécification multidiffusion IP, comme ICMP, pour les connexions unidifussion. IGMP peut être utilisé pour la vidéo en ligne et les jeux, et permet une utilisation plus efficace des ressources lors de l'appui de ces utilisations.

Interrogateur IGMP

Un routeur envoie des messages de requête IGMP sur un lien particulier. Ce routeur est appelé interrogateur.

IP

IP est un acronyme qui signifie le protocole Internet (*Internet Protocol*). C’est un protocole utilisé pour communiquer des données à travers un réseau internet.

IP est un système « meilleur effort », ce qui signifie le paquet d'informations envoyé est assuré d'atteindre sa destination dans le même état dans lequel il a été envoyé. Chaque périphérique connecté à un réseau local (LAN) ou un réseau étendu (WAN) possède une adresse de protocole Internet, cette adresse IP est utilisée pour identifier le dispositif unique parmi tous les autres appareils connectés au réseau étendu.

La version actuelle du protocole Internet est IPv4 qui a des adresses de protocole Internet de 32 bits créant ainsi la possibilité de quatre milliards d'adresses uniques. Ce nombre est considérablement réduit par la pratique des *webmasters* de s’approprier des adresses en gros blocs dont la majeure partie n’est pas utilisée. Il y a un mouvement assez important qui travaille vers l'adoption d’une nouvelle version du protocole Internet, IPv6. Cette version aurait des adresses de protocole Internet de 128 bits. Ce nombre peut être représenté à peu près par un trois avec 39 zéros. Toutefois, l'IPv4 est toujours le protocole de choix pour la plupart de l'Internet.

Gardien de source IP

IP Source Guard est une caractéristique sécuritaire utilisée pour restreindre le trafic IP sur les ports de surveillance DHCP non fiables en filtrant le trafic sur la base de la table de surveillance DHCP ou d'une configuration manuelle de liaisons IP. Il aide à prévenir des attaques par usurpation d'IP quand un hôte tente d'usurper et d'utiliser l'adresse IP d'un autre hôte.

L

LACP

LACP est un protocole standard IEEE 802.3ad. Le *Link Aggregation Control Protocol*, permet le regroupement de

plusieurs ports physiques pour former un seul port logique.

LLDP

LLDP est un protocole standard IEEE 802.1ab.

Le *Link Layer Discovery Protocol* (LLDP) spécifié dans cette norme permet aux stations attachées à un LAN IEEE 802 d'annonceré à d'autres stations rattachées au même LAN IEEE 802, les principales capacités fournies par le système intégrant cette station, l'adresse ou les adresses de gestion de l'entité ou les entités qui assurent la gestion de ces capacités, et l'identification du point de stations d'attachement au LAN IEEE 802 requis par cette entité ou ces entités de gestion. Les informations diffusées par l'intermédiaire de ce protocole sont stockées par ses destinataires dans un *Management Information Base* (MIB), ce qui rend possible que l'information soit accessible par un système de gestion de réseau (NMS) en utilisant un protocole de gestion tel que le *Simple Network Management Protocol* (SNMP).

LLDP-MED

LLDP-MED est une extension de IEEE 802.1ab et est défini par l'association de l'industrie des télécommunications (TIA-1057).

M

MAC Table (Table MAC)

L'échange de de trames est basée sur l'adresse DMAC contenu dans la trame. Le commutateur construit une table qui mappe les *MAC addresses* pour changer de ports pour savoir vers quels ports les trames devraient aller (basé sur l'adresse DMAC dans la trame). Ce tableau contient des entrées à la fois statiques et dynamiques. Les entrées statiques sont configurées par l'administrateur du réseau si l'administrateur veut faire un mappage fixe entre l'adresse DMAC et les ports du commutateur.

Les trames peuvent aussi contenir une *MAC adresse* (adresse SMAC), qui indique la *MAC address* de l'équipement qui envoie la trame. L'adresse SMACC est utilisée par le commutateur pour mettre à jour automatiquement la table de MAC avec ces adresses MAC dynamiques. Les entrées dynamiques sont retirées de la table MAC si aucune trame avec l'adresse correspondante SMAC n'a été observée après une durée configurée.

Mirroring (miroir)

Pour le débogage des problèmes de réseau ou surveiller le trafic du réseau, le commutateur peut être configuré pour dupliquer les trames à partir de plusieurs ports à un port miroir. (Dans ce contexte, dupliquer une trame équivautr à copier la trame.)

Les trames d'entrée (source) et de sortie (destination) peuvent être mises en miroir sur le port miroir.

N

Négociation automatique

La négociation automatique est le processus dans lequel deux dispositifs différents établissent le mode d’opération et les paramètres de vitesse qui peuvent être partagés par ces dispositifs pour une liaison.

P

PD

PD est un acronyme pour *Powered Device*. Dans un système AvE (PoE)> la puissance est livrée à partir d'un PSE (*Power Sourcing Equipment*) à un périphérique distant. Le périphérique distant est appelé un PD.

PHY

PHY est une abréviation pour *Physical Interface Transceiver* et est le dispositif qui met en œuvre la couche physique Ethernet (IEEE-802.3).

PING

Ping est un programme qui envoie une série de paquets sur un réseau ou sur Internet vers un ordinateur spécifique afin de générer une réponse de l'ordinateur. L'autre ordinateur répond avec un accusé réception des paquets. Ping a été créé pour vérifier si un ordinateur spécifique sur un réseau ou sur Internet existe et est connecté.

Ping utilise le protocole de message de contrôle d’Internet (*Internet Control Message Protocol*) (ICMP) des paquets. La demande PING est le paquet de l'ordinateur d'origine et la réponse PING est le paquet de réponse de la cible.

PoE

PoE est un acronyme qui signifie alimentation sur Ethernet (*Power Over Ethernet*).

Power Over Ethernet est utilisé pour transmettre l'énergie électrique vers des dispositifs distants avec des câbles Ethernet standards. Ce pourrait par exemple être utilisé pour alimenter des téléphones IP, des points d'accès LAN sans fils et autres équipements où il serait difficile ou coûteux de les brancher à l'alimentation principale.

Policier

Un policier peut limiter la bande passante des cadres reçus. Il est localisé devant la queue d’entrée.

Port de routeur

Un port de routeur est un port sur un commutateur Ethernet qui conduit un commutateur vers un dispositif de multidiffusion.

Priorité de la balise

La priorité du tag est un champ à 3 octets stockant le niveau de priorité du cadre 802.1Q.

Q

QCE

QCE est un acronyme pour *Qos Control Entry*. Il décrit la classe de QoS associé à un ID QCE particulier.

Il y a six types de trames Ethernet: QCE, VLAN, Port UDP / TCP, DSCP, TOS, et priorité d'étiquette. Les trames peuvent être classées par l'une des 4 classes de QoS différentes: "Faible", "Normal", "Moyen", et "Haute" pour les applications individuelles.

QCL

QCL est un acronyme pour *Qos Control List*. C'est la table de la liste des QCEs contenant les entrées de contrôle qui permettent de classer, dans une classe spécifique QoS, les objets de trafic spécifiques.

Chaque objet du trafic accessible contient un identifiant de son QCL. Les privilèges déterminent l'objet de trafic spécifique à la classe QoS spécifique.

QoS

QoS est un acronyme pour la *Quality of Service*. Il s'agit d'une méthode pour garantir une relation entre la bande passante des applications individuelles ou des protocoles.
Un réseau de communication transporte une multitude d'applications et de données, y compris la vidéo haute qualité et des données sensibles aux délais telles que la voix en temps réel. Les réseaux doivent fournir des services sécurisés et prévisibles, mesurables, et parfois garantis.

La réalisation de la QoS requise devient le secret d'une solution d'affaires de bout en bout réussie. Par conséquent, la qualité du service est l'ensemble des techniques permettant de gérer les ressources réseau.

R

RSTP

En 1998, l'IEEE avec le document 802,1w a présenté une évolution du STP: le *Rapid Spanning Tree Protocol*, qui assure une convergence plus rapide du *Spanning Tree*, après un changement de topologie. La norme IEEE 802.1D-2004 intègre désormais le RSTP et les STP désuets, tout en étant en même temps compatible avec le système STP.

S

SHA

SHA est un acronyme pour *Secure Hash Algorithm*. Elle a été conçue par la *National Security Agency* (NSA) et été publiée par le NIST en tant que norme *US Federal Information Processing*. Les algorithmes de hachage calculent une représentation numérique de longueur fixe (connu comme un condensé de message) d'une séquence de données d'entrée (le message) de n'importe quelle longueur.

STP

Spanning Tree Protocol est un protocole *OSI layer-2* qui assure une topologie sans boucle pour n’importe quel LAN ponté. Le protocole original STP est maintenant dépassé par RSTP.

T

TCP

TCP est un acronyme pour *Transmission Control Protocol*. Il s'agit d'un protocole de communication qui utilise le protocole Internet (IP) pour échanger des messages entre des ordinateurs.
Le protocole TCP garantit la livraison fiable et en ordre des données de l'expéditeur au destinataire et distingue les données pour les connexions multiples par des applications simultanées (par exemple, serveur Web et serveur de messagerie) fonctionnant sur le même hôte.
Les applications sur les hôtes en réseau peuvent utiliser TCP pour créer des connexions à une autre. Il est connu comme un

protocole orienté connexion, ce qui signifie que la connexion est établie et maintenue jusqu'à ce que le ou les messages qui doivent être échangées par les programmes d'application à chaque extrémité ont été échangés. TCP est responsable de s'assurer qu'un message est divisé en des paquets IP qui assure la gestion et le réassemblage des paquets de retour dans le message complet à l'autre extrémité.

Les applications en réseau courantes qui utilisent TCP comprennent le *World Wide Web* (WWW), courriel, et *File Transfer Protocol* (FTP) .

ToS

ToS est un acronyme pour *Type of Service*. Il est implémenté comme le contrôle de priorité Ipv4 ToS. Il est entièrement décodé pour déterminer la priorité du champ de 6 bits ToS dans l'en-tête IP. Les 6 bits les plus significatifs du champ ToS sont entièrement décodées en 64 possibilités, et le code singulier qui en résulte est comparée au bit correspondant dans le bit de commande de priorité IPv4 ToS (0 ~ 63).

U

UDP

UDP est un acronyme pour *User Datagram Protocol*. Il s'agit d'un protocole de communication qui utilise le protocole Internet (IP) pour échanger des messages entre des ordinateurs.
UDP est une alternative à *Transmission Control Protocol* (TCP) qui utilise le protocole Internet (IP). Contrairement à TCP, UDP ne fournit pas le service de diviser un message en datagrammes de paquets, et UDP ne fournit pas de réassemblage et le séquençage des paquets. Cela signifie que le programme d'application qui utilise le protocole UDP doit être capable de faire en sorte que l'intégralité du message est arrivé et est dans le bon ordre. Les applications réseau qui veulent gagner du temps de traitement parce qu'ils ont de très petites unités de données à échanger peuvent préférer UDP pour le protocole TCP.
UDP fournit deux services non fournis par la couche IP. Il fournit les numéros de port pour aider à distinguer les demandes des différents utilisateurs et, éventuellement, une capacité de contrôle pour vérifier que les données sont arrivées intactes.
Les applications réseau les plus courantes qui utilisent UDP comprennent le *Domain Name System* (DNS), les applications de diffusion de média telles que l'IPTV, la Voix sur IP (VoIP), et *Trivial File Transfer Protocol* (TFTP).

Priorité de l'utilisateur

Priorité utilisateur est un champ de 3 bits stockant le niveau de priorité pour la trame 802.1Q.

V

VLAN

Virtual LAN. Procédé pour restreindre la communication entre les ports d'un commutateur. Les VLAN peuvent être utilisés pour les applications suivantes:

VLAN unaware switching: Il s'agit de la configuration par défaut. Tous les ports sont ignorants du VLAN avec ID de Port VLAN 1 et les membres de VLAN 1. Cela signifie que les adresses MAC sont apprises dans le VLAN 1, et le commutateur ne pas supprimer ou insérer des étiquettes VLAN.

VLAN aware switching: Ceci est basé sur la norme IEEE 802.1Q. Tous les ports sont conscients du VLAN. Les ports connectés à des commutateurs VLAN conscients sont membres de plusieurs réseaux locaux virtuels et transmettent des trames marquées. Les autres ports sont membres d'un VLAN, mis en place avec ce port ID VLAN, et transmettent des trames non marquées.

Provider switching: Ceci est également connu en tant que commutation *Q-in-Q*. Les ports connectés aux abonnés sont ignorants du VLAN, membre d'un VLAN, et mis en place avec ce port unique d'ID VLAN. Les ports désservis par le prestataire de services sont conscients du VLAN, membre de plusieurs VLAN, et mis en place pour marquer toutes les trames. Les trames non marquées reçues sur un port d'abonné sont transmises au port fournisseur avec une seule étiquette VLAN. Les trames marquées reçues sur un port d'abonné sont transmises au port avec une étiquette de VLAN double.

VLAN ID

VLAN ID est un champ de 12 bits qui spécifie le VLAN auquel le cadre appartient.

VLAN Privé

Dans un VLAN privé, la communication entre les ports dans un VLAN privé n’est pas permise. Un VLAN peut être configuré en tant que VLAN privé.